

**Success Factors of Information Security Management:  
A Comparative Analysis between Jordanian and Finnish  
Companies**

**By Sami Abu-Zineh**

**M.Sc. Thesis in Accounting  
The Swedish School of Economics and Business Administration –  
HANKEN**

**2006**

## HANKEN-The Swedish School of Economics and Business Administration

<b>Department:</b> Accounting	<b>Type of work:</b> Master of Science Thesis
<b>Author:</b> Sami Abu-Zineh	<b>Date:</b> 15.05.2006
<b>Title of Thesis:</b> SUCCESS FACTORS OF INFORMATION SECURITY MANAGEMENT: A COMPARATIVE ANALYSIS BETWEEN JORDANIAN AND FINNISH COMPANIES	
<p><b>ABSTRACT</b></p> <p>Managing the ever-growing amount of information assets around the world has become a major challenge for everyone, from individuals to large global organizations. The purpose of this research paper is to make comparative analysis between Jordanian and Finnish companies regarding the importance of success factors of ISM.</p> <p>The introduction section discusses information security management and illustrates countries development towards information security. The theoretical part discusses in detail the evolution of ISM and documents background information of studied countries.</p> <p>The purpose of the empirical study has been to make a comparative analysis between studied countries regarding the importance of factors that are responsible for success of ISM. Moreover, this study also ranks the success factors of ISM from most important to least important. An online survey was conducted and out of 152 companies in Finland and 85 in Jordan, twenty eight companies (33%) in Jordan and thirty companies (20%) in Finland have filled out the survey.</p> <p>The importance of these factors based on a comparative analysis between Jordanian and Finnish companies was explored. Furthermore, this study ends with classifying these factors from top important to least important factor and some practical suggestions are introduced.</p>	
<b>Keywords:</b> Information Security, Information Security Management (ISM), Information Security Policy (ISP), Information Systems (IS)	

## Acknowledgements and Dedication

Since this thesis is the first science paper I have written, I would dedicate it to my parents for their great supportiveness during the period of my study in Finland

# Table of Contents

<b>1. INTRODUCTION.....</b>	<b>I</b>
1.1 Background.....	1
1.2 Research Objectives.....	2
1.3 Research Structure .....	3
<b>2. LITERATURE REVIEW .....</b>	<b>4</b>
2.1.Objectives and structure of chapter .....	4
2.2 Information Security .....	4
2.3 Objectives of Information Security .....	5
2.4 Information Security Management (ISM).....	5
2.6 Contributions of Theoretical and Empirical Studies in Success Factors of ISM .....	9
2.6.1 Theoretical Studies.....	9
2.6.2 Empirical studies.....	14
2.7 Summaries and discussion of chapter.....	17
<b>3. RESEARCH MODEL .....</b>	<b>19</b>
3.1 Objectives and structure of chapter .....	19
3.2 Studied Countries.....	19
3.2.1 Finland.....	20
3.2.2 Jordan.....	21
3.2 Success Factors of Information Security Management .....	24
3.2.1 Top management support .....	24
3.2.2 Information security policy (ISP).....	25
3.2.3 Job Responsibilities.....	27
3.2.4 Motivation of Employees.....	28
3.2.5 Awareness and Training programs.....	29
3.2.6 Compliance with information security international standards.....	30
3.2.7 Using services of information security external advisors.....	31
3.3 Summary and conclusion of chapter.....	32
<b>4. RESEARCH METHODOLOGY .....</b>	<b>34</b>
4.1 Objectives and structure of the chapter.....	34
4.2 Research Hypotheses .....	34
4.3 Data Gathering.....	37
4.3.1 Sample description.....	37
4.3.2 Survey Description.....	38
4.3.3 Survey questions that used for testing Hypotheses.....	39
4.4 Total of Received Responses .....	40
<b>5. EMPIRICAL RESULTS .....</b>	<b>41</b>
5.1 Objectives structure of the chapter .....	41
5.2 Analysing method.....	41
5.3 Respondent Companies Background Information.....	42

5.3.1 Number of Employees.....	42
5.3.2 Independent Department of Information Security Management.....	43
5.3.3 Years of Experience of the Respondents.....	44
5.4 Description of Data, Testing Hypotheses of the Comparative Analysis.....	46
5.4.1 Top Management Support.....	46
5.4.2 Information Security Policy (ISP).....	51
5.4.3 Job Responsibilities.....	55
5.4.4 Motivation of Employees.....	57
5.4.5 Awareness and Training programs.....	61
5.4.6 Compliance with information security international standards.....	64
5.4.7 Using services of information security external advisors.....	68
5.5 Testing second part of hypotheses (importance of the success factors of ISM).....	72
<b>6. CONCLUSION .....</b>	<b>74</b>
6.1 Validity, Reliability and Generalizability .....	74
6.2 Discussion and Summery .....	74
6.3 Analysis of study contribution .....	78
6.4 Further research suggestions .....	78
<b>7. REFERENCES.....</b>	<b>79</b>
<b>APPENDIX A.....</b>	<b>82</b>
<b>APPENDIX B.....</b>	<b>86</b>
<b>APPENDIX C.....</b>	<b>92</b>

## Table of Figures

<b>Figure 2- 1</b>	Model of Information security effectiveness (Kankanhalli et.al, 2003)..	17
<b>Figure 3- 1</b>	Success factors of Information Security Management (ISM).....	24
<b>Figure 3- 2</b>	ISM and Job Responsibilities.....	28
<b>Figure 5- 1</b>	Information Security Management Department.....	44
<b>Figure 5- 2</b>	Years of Experience of the Respondents.....	45
<b>Figure 5- 3</b>	ISM and Corporate Strategies .....	47
<b>Figure 5- 4</b>	Reviewing and approving the ISM plans by the top management.....	48
<b>Figure 5- 5</b>	Importance of the top management support.....	49
<b>Figure 5- 6</b>	Availability of the ISP .....	52
<b>Figure 5- 7</b>	Importance the ISP .....	53
<b>Figure 5- 8</b>	Support and involved of the end-users in the ISP .....	54
<b>Figure 5- 9</b>	Information security is everyone's job.....	55
<b>Figure 5- 10</b>	Importance of the job responsibilities .....	56
<b>Figure 5- 11</b>	Importance of the motivation of the employees.....	58
<b>Figure 5- 12</b>	Reward and Appreciation Systems and the Motivation Level.....	59
<b>Figure 5- 13</b>	Availability of the reward and appreciation systems .....	60
<b>Figure 5- 14</b>	importance of the awareness and training programs .....	62
<b>Figure 5- 15</b>	Availability of the awareness and training programs .....	63
<b>Figure 5- 16</b>	Managing the awareness and training programs .....	64
<b>Figure 5- 17</b>	Importance of compliance with information security international standards .....	65
<b>Figure 5- 18</b>	The information security international standards implementation.....	67
<b>Figure 5- 19</b>	Competitive advantage and adopting the information security international standards.....	68
<b>Figure 5- 20</b>	Using the service of the external parties for managing information security.....	69
<b>Figure 5- 21</b>	Importance of using service s of information security external advisor.....	70
<b>Figure 5- 22</b>	Using the services of the recruitment agencies. ....	71

## Table of Tables

<b>Table 3- 1</b>	Economical and Technological indicators of studied countries .....	22
<b>Table 3- 2</b>	Information security standards .....	31
<b>Table 4- 1</b>	Survey questions used for hypotheses.....	39
<b>Table 4- 2</b>	Data Gathering results.....	40
<b>Table 5- 1</b>	Number of the employees of respondent companies.....	42
<b>Table 5- 2</b>	T-Test Statistics of Years of Experiences .....	45
<b>Table 5- 3</b>	Independent Sample Test of Years of Experience.....	46
<b>Table 5- 4</b>	Chi-Square test of Top management support factor .....	50
<b>Table 5- 5</b>	Cross tabulation of Top Management support factor for Jordan and Finland .....	51
<b>Table 5- 18</b>	Statistical results of testing second part of hypotheses .....	73
<b>Table 6- 1</b>	Summery of tested hypotheses.....	75

# 1. Introduction

## 1.1 Background

Information security has become one of the most important issues of any organization. Thus, the organization needs to ensure that their information assets are properly protected and maintains high level of information security. An acceptable level of information security can only be introduced and maintained if the correct set of security controls, both procedural and technical, are identified, implemented and maintained (Solms R. 1998).

Managing information security plays an essential part in the overall information security environment. Unmanaged information security can never be secured (Finne T. 1998, pp303-307). Therefore, the information assets must be adequately secured in order to achieve the objectives of ISM and the objectives of the organization. There are many critical factors in ISM that need to be addressed appropriate attention. These factors should be seriously taken into account, and taking care of any other factor is definitely of less importance (Hinson G. 2003).

Information security management should commit its roles and make them convincing for top management. Mainly, ISM obligation is to ensure that the security requirements imposed on the systems will adequately protect organizations' resources and data. Another obligation of ISM is to ensure that the system is operated in such a manner that satisfies the security requirements and reports significant deviations in security. (Marshall et.al. 1995)

ISM is stream of management activities that aims to protect information assets and secure the framework of organization where the information system is operated (Solms R. 1998, pp174-177). It implies that assessment of information assets might differ from organization to organization depending on the geography and business scope of the organization. Therefore, organizations located in developed countries with relatively advanced organizational development might pay more attention towards protecting information assets as compared to their counterparts in developing

countries. In developing countries the organizations may not pay high attention towards protecting information assets for a number of reasons. For example, high percentage of IT illiterate population might deter organizations in developing countries to overlook their information security needs. Thus, the threats to attack information assets would be less in developing countries compare to developed countries that have high percentage of IT literate population. On other hand, misuse and loss of information assets in developing countries might be higher than in developed countries.

Developed and developing countries are differ from each other in levels of economic development, technological know how and education. These differences might be responsible for causing different point of views towards information assets and managing information security.

To the best of my knowledge, not much work has been done in understanding how professionals in developed and developing countries view information assets and information security requirements. In this paper I will be covering one aspect of this area, namely comparative analysis of ISM's success factors in developing and developed countries. I have chosen Jordan as a representative country for developing economies and Finland as representative of developed countries.

## 1.2 Research Objectives

The objective of my study is to make a comparative analysis between Jordanian and Finnish companies regarding the importance of factors that are responsible for success of Information Security Management. As discussed earlier, these countries have different levels of economic, technological, and educational development therefore; I expect a significant difference between these two countries regarding the importance of success factors of ISM. Moreover, this study also ranks the success factors from most important to least important.

## 1.3 Research Structure

This research has been divided into seven chapters. Chapter 1 is an introduction of information security management and the objectives of the research. Chapter 2 discusses information security and its objectives. Various definitions of ISM have also been discussed and introduced. The contributions of theoretical and empirical studies have been reviewed and analyzed in context of success factors of ISM.

Chapter 3 introduces the research model of my study. The research model consists of two parts. First part introduces background information of the studied countries and discusses the economic, technological, educational, and organizational situations of these countries. Second part introduces the success factors of ISM. The model consists of seven success factors of ISM (see figure 3-1).

Chapter 4 consists of the research methodology. Fourteen hypotheses have been developed in this study. Seven hypotheses will be used for comparative analysis, and the another seven hypotheses will be used for measuring importance of these factors for ISM's success. This chapter also introduces the description of data gathering process (Sample and Survey descriptions), survey questions used for testing hypotheses, and the statistical calculations for total of received responses. Chapter 5 contains of empirical results. This chapter consists of two parts. First part analyses and discusses background information of the respondent companies such as, number of employees, independency of ISM department and the years of experience of respondents. Second part describes the analyses and tests the research hypotheses.

Chapter 6 addresses the issues of validity, reliability and Generalizability, discussions and summary of research results, and analyses of the contribution of this study along with suggestions for further researches. Chapter 7 consists of alphabetically arranged references. Three appendixes are created. Appendix A contains the survey questionnaire, appendix B contains the tables that are generated by Chi-square test for comparative analysis, and appendix C has some other tables generated for further analysis to support the description of data.

## **2. Literature Review**

### **2.1. Objectives and structure of chapter**

ISM and its success factors have been discussed in different articles, books, and information security international standards web sites. This chapter reviews a number of theoretical and empirical studies to discuss definitions of ISM and factors that have been considered as having important influence on managing information security. Some of these factors will be discussed in greater details.

This chapter consists of two sections. First section introduces background of definitions of information security and its objectives. Furthermore, this section consists of definitions, modules and frameworks of ISM. Second section discusses the contributions of theoretical and empirical studies towards success factors of ISM.

### **2.2 Information Security**

Security for a companies has many forms and variations such as; information security, operation security, production security, personnel security and computer security etc. Importance of information security arises when the information assets of organizations are exposed to loss or misuse (Finne T. 1998; Solms R. 1998 pp 174-177).

Information security comprises of techniques, technical measures, and administrative measures that are used to protect information assets against unauthorized acquisition, damage, disclosure, manipulation, modification and loss or misuse (Eloff & Eloff 2003). The U.S. National information systems security glossary defines information security as: the protection on information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of services to unauthorized users. Including these measures necessary to detect, document, and counter such threats (Hone & Eloff 2002). This definition implies that information security is not only a

technical issue, but also a management issue of highest importance, whose main goal is to offer a secure information environment.

“The scope of information security is the protection of all spoken, printed, and automatically recorded information owned, in the custody of, or used by individuals and organizations. The scope also includes the protection of all resources that are the means of creating processing, transmitting, storing, using, displaying or controlling, and controlled environment facilities, communication networks, information workers, peripheral equipment, recording and storage media” (Finne T. 1998 pp 53-56). Therefore information security is an interdisciplinary concept that contains a host of issues related to the information life cycle.

## 2.3 Objectives of Information Security

Information security has been considered to consist of the following three main objectives: *information confidentiality, integrity, and availability*. Confidentiality refers to the prevention of unauthorized disclosure of information, integrity points to the prevention of unauthorized modification of information, and availability reflects withholding of information or resources (Finne T. 1998 pp 53-56; Mitchell et.al 1999).

- The confidentiality keeps valuable information only in the hands of those people who are intended to see it.
- The integrity is about maintaining the value and the state of information, which means that it is secured from unauthorized modification, so that the information has value if we know that it is correct.
- The availability of the information is the information available when it is needed.

## 2.4 Information Security Management (ISM)

Information security management is stream a of management activities that aims to protect the information assets and secure framework within the organization where information system is operated. Hence, one of the main aims of ISM is to minimize the risks that information assets may face (Solms R. 1998 pp 174-177).

ISM process is an iterative process with feedback and continuous improvements. It includes several processes starting from identifying information security needs, followed by necessary strategies to meet these needs and measuring of results in order to improve ISM (Bjorck F. 2001). Eloff & Eloff (2003) defined ISM process as "Plan-Do-Check-Act" where management identifies the processes to be implemented, verifies whether all implemented processes are screened or not, and tack action according to the outcome and feed back.

Information security management is a crucial part of overall information security (Finne T. 1998 pp 80-83). Recent developments of information systems have made managing information security tough and complex. Accordingly, it requires management to adopt strategic point of view and place more faith in architectural and environmental controls of ISM.

Eloff & Eloff (2003) proposed two aspects of ISMS: Process of ISMS and Products of ISMS. The process of ISMS is an issue focusing on planning and implementing management practices, as well as the procedures and processes that are used to establish and maintain information security. The process of ISMS starts by defining and implementing the controls and guidelines followed by assessing these controls and guidelines in order to determine whether they are compliant with the international standards. This aspect matches with the concept "Plan-Do-Check-Act". As well as, all

The second aspect is the product of ISMS, which is a management system used by organization to evaluate software products. Product evaluation is the process whereby a specific product or system is subject to a detailed series of tests to determine whether it satisfies a predefined set of requirements. Most probably the product ISMS is tested by third party. Combining the products of ISMS with the processes of ISMS can be done by defining the requirements of code-of-practices include in ISO 17799 and by building a framework to facilitate a relationship between processes and products.

Information Security Management System (ISMS) is used for establishing and maintaining a secure information systems environment. It takes into account policies, standards, guidelines, codes-of-practices, technology, human issues, legal, and ethical issues during establishing effective ISMS (Eloff & Eloff 2003). Furthermore, there are several perspectives used to approach ISM:

- Strategic perspective addresses the corporate governance, policies and pure management issue,
- Human perspective approach addresses the issues of security culture, awareness, training, ethics and other human issues, and
- Technology perspective approach is focused on the hardware and software products.

These definitions have focused on the importance of information assets and proper management of these assets. Solms (1998) has defined ISM as a stream of activities which aims to minimize the risk to lowest level (Solms R. 1998 pp 174-177). While, Bjorck (2001) defined ISM as a mechanism used to define strategies to meet the information security requirements and measure these strategies. These definitions complement the definition put forward by Eloff & Eloff (2003) where they defined the ISM as ISMS that consists of intelligent mix of several issues surrounding ISM.

Solms (1996) introduced the second generation of ISM by defining the imperative need for information security evaluation schemes. He mentions how a lot of organizations and their partners are willing to share some parts of their systems together in order to enhance a business environment. Therefore the second generation of ISM illustrates the following schemes that should adopt by the organization to evaluate the level of information security.

- Trusted Computer Security Evaluation Criteria scheme (TCSEC): It is concerned about products evaluation. It addresses following three aspects of evaluation criteria: *functionality* (refers to the features of a system), *effectiveness* (used to

ensure that the used mechanisms are appropriate for the given security requirements), and *assurance* (diligence of the evaluation).

- ISO 9000: It is a series of international quality standards that mainly applied to check the quality of management systems and the processes of products. ISO 9000 addresses the information security issues such as policies, risk analysis, and continuity planning.
- Code of Practice: The CoP of ISM is a reference document for managers and employees who are responsible for initiating, implementing and maintaining information security within their organizations. The aims of CoP are to provide a common basis for companies to develop, implement, and measure effective security management practice and enhance the confidence level in the companies.
- Information security self evaluation scheme can be used by the organization itself to evaluate whether they have an adequate protection or not. This scheme is similar to the checklist method that is used by the management to test the effectiveness, functionality and availability its information security controls.

Using these schemes is an attempt to enhance confidence level between the organizations that would help the organization to keep information asset highly secure.

Finne (1998) introduced a conceptual framework of ISM by viewing how ISM fits into the context of risk management. His framework studies how ISM may be used to assess the economic losses that might be caused by breaches of information systems. His work helps management to understand and use of security tools in order to protect information asset at all levels of the company in context of risk management (Finne T. 1998 pp 303-307).

Kwok & Longley (1999) developed the Risk Data Repository model (RDR) that aims to manage information security data by facilitating risk analysis. His model is used to comprise the following three important domains:

- Environment: It consists of the Equipments, Building, Staff etc. which support the information processing system

- Platform: It defines the logical description of the information processing system and its defence.
- Assets: they are the assets that should be protected to avoid misuse and flaws.

## 2.6 Contributions of Theoretical and Empirical Studies in Success Factors of ISM

The following section discusses the contributions of theoretical and empirical studies in defining successful factors of ISM.

### 2.6.1 Theoretical Studies

Lau (1998) introduced numerous factors that have influence on success of ISM. Information security managers should take care of all these factors to build an adequate information security system and play activist role to achieve ISM objectives. Lau introduced two factors into his study: situation of users and risk assessment. He advocates that both of these factors should fairly be evaluated during the information security development process. He classifies aims of information security on the bases of risk to which information assets are exposed to. Lau (1998) suggested the following recommendations to minimize the risk of potential damage depending on specific measures and needs of information security:

- Enhance prevention measures by patching existing security holes.
- Anticipating development issues and analyzing current needs to conceive complete security solutions.
- Deploying corrective measures to ensure that detected intrusion teaches you something advantageous.

“If we don’t know what to do, then how can we do it?” Nosworthy (2000) tried to find convincing answer for this question by introducing the information security policy and some factors that play an important role for success of ISM. The author introduced several factors that have a negative effect on ISM implementation. These factors are:

- “It will never happen for us”, this axiom used by an organization that still have a mindset because they never had problems.
- Emphasizing just on IT issue not on the business
- Reluctance to release resources
- Lack of understanding for information security
- Lack of awareness for responsibility and ownership
- Non-acceptance of importance of security education and training
- No training budget

He assembled the following factors that should be considered during ISM implementation.

**Table 2- 1** *Factors that should be considered during the ISM Implementation*

<b>Factor</b>	<b>Author's Perspective</b>
People	People make things happened. ISP is useless without people.
Culture	Organizational culture plays a major role in ISM. ISM plan used for manufacturing company should not be the same as the one used for services company.
People's attitude	People's attitudes depend on the way people view information security and what it means to the organization
Security education and training	Employees can not make ISM plan done without sufficient education and training.
Ownership	Ownership illustrates that person owns information and has responsibility towards implementing information security.

Job descriptions	Job description should state responsibilities toward information security, document training and educational requirements.
------------------	--

Eloff & Eloff (2003) mentioned that the optimal method to combine ISMS' product and process is to define the requirements of Code of practice. The main source for this CoP is the British standard (BS7799).

The Code of Practice (CoP) is defined and introduced in the context of ISM implementation based on a collection of the best information security practices that in general are used in many international organizations (Solms R. 1998 pp 224-225; Solms R. 1999). The main objective of the CoP is to provide a common basis for companies to develop, implement, and measure their information security practices as well as to enhance the confidence between the organizations. This complies with main goals of information security to ensure the business continuity by preventing and minimizing the impact of security incidents (Solms R. 1996; Farahmand et.al 2003).

The Codes of Practice are consisting of ten categories that should be present in most organizations;

1. Information Security policy
2. Security organization System development and maintenance
3. Business contingency planning
4. Compliance with security policy and other international standards

Solms & Solms (2004) demonstrated ten important aspects to avoid any serious flaws or mistakes, which could happen during evaluation and implementation of information security management process. Many other studies introduced these aspects from different point of views, and most of these aspects play critical roles to keep the information security environment adequately secured.

1. Information security is a corporate governance responsibility. If the management are not performing and exercising the reasonable carefulness expected by them, it may open themselves up to serious personal and corporate responsibilities
2. Protection of information is a business issue, rather than technical issue. Solving information security related problems can't be managed by technical means alone. A proper, direct, continuous support of executive management, enhancement of information security consciousness, and awareness play a main role in minimizing and addressing the information security problems.
3. Information security governance is a multi-dimensional discipline. Many dimensions should be defined in the context of information security. These different dimensions must collectively contribute toward a security environment
4. Information security plan must be based on identified risks. The company must use information security as a countermeasure to protect itself from the threats associated with company's information resources, and they must define the serious risks and pay adequate attention to manage it, rather than tacking care and spending money on risks which may not really be crucial. In addition, risk assessment has to aim on identifying, measuring, and controlling uncertain events in order to minimize loss and optimize the return of the money invested for information security purpose.
5. Important role of international best practices for information security governance: Nobody will re-invent the information security wheel, because this wheel has been developed as well as documented and should be used as such. The new information security mangers should rely on the experience that had been documented in wide set of documents, mainly referred to as standards and guidelines. Spending money and time to arrive solutions which had already been documented is absolutely irrational.
6. A corporate ISP is absolutely essential. The information security policy is the heart and basis of any successful ISM plan. The ISP shows procedures and standard used by information security management and clarifies the executive management commitment toward information security.
7. Information security compliance enforcement and monitoring is absolutely essential. The monitoring and measurement tools should show the compliance of polices with standards and guidelines. The real time reports should be issued

frequently to avoid abuses and breaches that could be done by users. Moving information security toward stage to potential business partners may help a company getting new contacts. On the other hand, a lack of information security may result in loss of some market advantages.

8. Proper information security governance structure (organization) is absolutely essential. This dimension refers to information security responsibility that is posted for every body in the organization. The accountability for information security must be shared by all employees, not only the information security manager, and must be spelled out clearly and coherently into a proper organizational structure.
9. It is really important to keep information security awareness amongst users. The money dedicated for awareness programs ensure that the best portion of money is spent on information security. Users cannot be held responsible for security if they are not educated with such security problems and what they should do to prevent them.
10. Empowering information security manager with the infrastructure, tools and supporting mechanisms is a crucial issue. The information security manager may perform his/her job properly due to the complexity and the multi-dimensionality of information security. Hence, the management should take adequate care of this point otherwise they will open a company up to severe risks and the ISM's plans never get fully implemented

(Solms 1998 pp 224-225) exhibited several factors which are often critical to successful implementation of ISM:

1. Security objectives and activities must be conducted based on business objectives and requirements, and led by business management
2. There must be a visible support and commitment from top management
3. There must be a good understanding of security risk (threats and vulnerabilities) to company assets, and the level of security inside the organization.
4. Security must be effectively marketed to all managers and employees
5. Comprehensive guidance on security policy and standards must also be distributed to all employees and contractors.
- 5.

6. Assets classification and control
7. Personal security
8. Physical and environmental security
9. Computer and network management
10. System access control

### 2.6.2 Empirical studies

Mitchell et.al (1999) focused on investigating the human attitudes towards information security amongst key decision makers in commercial organization in UK. They found that the security of corporate information is extremely important for ensuring business continuity. Many organizations are not proactively tackling ISM seriously which made them vulnerable to security risks. The main reasons for the lack of this action are: awareness of information security threats is limited; management and awareness of information security is intense just about the IT department; electronic information is viewed as an intangible business asset; potential security risks of internet access have not been fully assessed; and most companies have not yet encountered security problems. Therefore they are not willing to invest in security measures.

They suggested that the companies should consider the following recommendations in order to avoid any misuse or lose of information asset:

- All the possible security exposures and quantification of potential costs should be based on a formal risk analysis
- Releasing ISM from being an IT- centric function
- Encouraging the view that information is a valuable corporate asset and must be given a special attention.

Bjorck (2001) described experiences and perspectives in term of critical factors vital to the ISM implementation and certification processes. The empirical side of his study focused on the certifications auditors' and information security consultants' experiences and insights concerning the implementation and certification of ISMS. Six factors were identified according to the Certifications auditors' perspective on implementation and certification of ISMS. These factors were:

1. Management commitment: this factor was the most one mentioned by the auditors respondent group
2. Well-structured project: this factor introduced by respondents, which mentioned the important role of structure in risk analysis and organizational responsibilities
3. Holistic approach: respondents emphasized on the ability of project members and other employees to see the full picture of whole business issue which allows them to obtain holistic view of all enterprise. This factor combined between information security and the organizations processes, so that the ISMS does not end at the security- or IT department.
4. Appreciating the need for information security: this factor was mentioned many times by respondents, and demonstrated the need for information security for whole organization. It is extend to cover all aspect of information systems.
5. Motivated employees: most of the answers focused on motivation of individuals participating in the ISMS project, such as project participants, project manager, and those responsible for different area in the organization.
6. Access to external competence: the ability to call for external competence when needed is an important factor which demonstrated the need for both experts and advisors in IT and information security

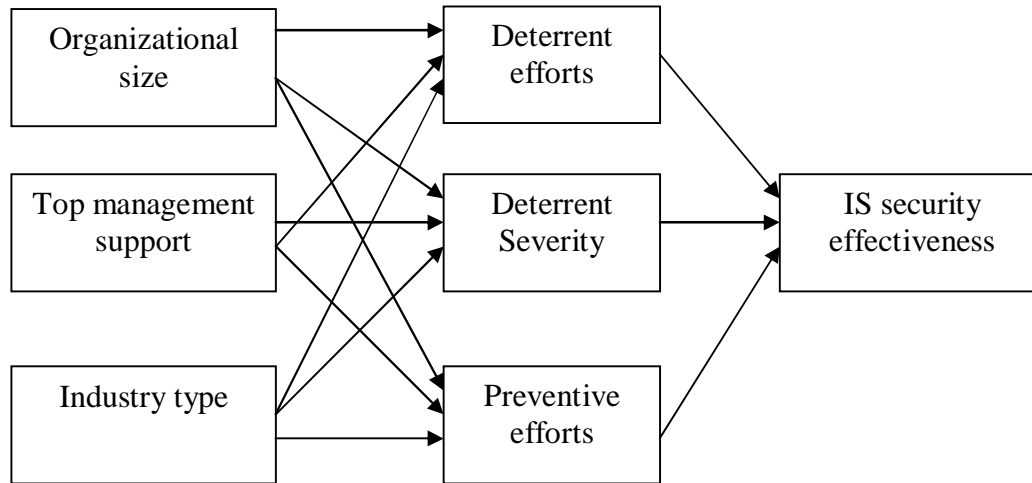
Another Six factors were defined regarding the information security consultants' perspective on implementing and certification of ISMS:

1. Project management capability: an efficient project management capability is essential for successful implementation ISMS, such as the need for active project members, an appropriate project organization and realistic time plan.
2. Commanding capability: this capability empowers the role of top management by defining and supporting the information security throughout management's awareness and involvement in information security.
3. Financial capability: located the needed resources in order to estimate costs realistically.
4. Analytic capability: this aspect focused on the importance of analytical capability in order to enhance ISMS by balanced policy grounded reality.

5. Communicative capability: the interacting process between information security manager and other parties is an important factor, and the information security efforts should not be stopped at the security manger desk.
6. Executive capability; developing ISPs is an important thing which contains all the security ideas, rules, controls, and procedures. These policies need to be done and put into practice. Furthermore, the employees should influence the IT ideas and other parts of the organization.

Kankanhalli et.al (2003) developed an integrative model of information security effectiveness. Small and medium-sized Singaporean enterprises were surveyed to examine the ability of the measures to protect against unauthorized or deliberate misuse of information assets by employees. Organizational factors such as organizational size, top management support, and industry type strongly influenced information security measures. The organizational size play critical role in adopting information security system, the smaller organizations suffer from lack of human, financial support and technical skills. Therefore, smaller organizations reap fewer benefits as comparative larger organization while implementing ISM.

Top management support was also found to be critical factor in successful implementation of ISM. The top management support represented through guidance during planning, participation during designing and involvement during deployment. In addition, the top management play main role of encouraging user attitude towards the use of ISP. Organizations in different industries tend to differ in terms of their requirements, uses and roles of ISM.



**Figure 2- 1** *Model of Information security effectiveness (Kankanhalli et.al, 2003)*

## 2.7 Summaries and discussion of chapter

Basically, many important success factors were introduced in the theoretical studies. Some of these factors have been tested and proofed into the empirical studies while several of these factors still not tested.

**Theoretically**, the second generation of ISM has defined several evaluation schemes where most of the organizations are willing to share their information based on such kind of these schemes (Solms R. 1996). Finne (1998 pp 50-53) introduced the conceptual framework of ISM to view how the ISM fits into the context of risk management. Kwok & Longley (1999) have defined the Risk Data Repository model that used to facilitate the risk analysis process by defining the external impacts on the operation systems. Eloff & Eloff (2003) described ISMS as an process that focuses on planning and implementation of management practices, while the product of ISM was described as organizations ability to evaluate software products.

All of these models and theories demonstrate the importance of the ISM for having a secure information environment. Thus many factors should be taken into account for successful implementation of ISM. Ignoring these factors will expose the information asset to high threats. Enhancing the prevention measures, developing security solutions and implementing corrective measures to increase the knowledge of users will make these factors more reliable to be success (Lau O. 1998).

**Empirically,** Mitchell et.al, (1999) focused on important of information security for ensuring business continuity. They defined the reasons that may make companies are not prepared for security incidents. Bjorck (2001) has investigated importance of several factors regard ISM in Sweden. Based on perspectives of certification auditors and information security consultants; six factors for each group of respondents have been classified. Kankanhalli et.al, (2003) have developed information security model. This model integrates three organizational factors (organization size, top management support, and industry type). This model demonstrates how these factors work together to have effectiveness information system security based on deterrent and prevention efforts.

I will introduce and discuss some of these factors into my study. I think these factors could not be recorded as success factors unless they have not a real effect on the success of ISM. After reviewing many recent studies regarding ISM, I just found a few empirical papers have tested some factors related to the ISM. This shortage of empirical studies gives me the right direction to test these success factors in light of success ISM implementation.

## **3. Research Model**

### **3.1 Objectives and structure of chapter**

Chapter 2 discusses a number of theoretical and empirical studies that discuss various issues concerning ISM. These studies identified quite few factors that are essential for ISM success. I have identified seven factors for this study that I consider to be of prime importance for success of ISM.

The aim of this study is to document any difference that might exist between Finland and Jordan regarding success factor of ISM. Therefore, I will begin by describing important facts about Finland and Jordan. Some of these facts might be responsible for creating difference these studied countries.

Two sections will be covered in this chapter. First section will discuss background of studied countries. Second section will discuss the success factors individually.

### **3.2 Studied Countries**

Information is considered as an important resource that enhances the development process in markets. Prior literature has identified that automated information systems are the main modules for socio-economic development. If and when coupled with appropriate communications infrastructure, information systems can cause countries to progress very rapidly.

Since the main objective of this study is to document a comparative analysis between Jordan and Finland, therefore background information about these countries is discussed below.

### 3.2.1 Finland

Finland is one of the EU countries with a population of 5.231 million for (2006), and population growth rate of .14%. Labor force in Finland was 2.61 million during 2005 and GDP per capita was \$30,600 for 2005 with growth rate of 2.2% ([www.cia.org](http://www.cia.org))

Finnish government has established different kinds of organizations to support innovation and business continuity. The international success of Nokia and many smaller high-tech companies has been seen as a proof of the competitiveness of the Finnish system.

In Finland, education and innovation are seen as important means to succeed in the global market. According to the world Fact-book ([www.cia.gov](http://www.cia.gov)); 100% of Finns are literate. The education system in Finland has been ranked as the first of the world towards meeting the needs of a competitive economy (IMD, The world Competitiveness Yearbook 2005).

Finnish companies have gone through a relatively large structural change over the past couple of decades. The volume of exports in 2005 was \$67.88 billions, which has grown very rapidly during the 1990s. The current prosperity is based largely on the global success of two clusters: forestry and IT. Both are good examples of Finns' skill in exploiting their expertise through cooperating and working together in areas such as R&D for everyone's common benefit ([www.cia.gov](http://www.cia.gov)).

By any indicators, Finland excels in the IT sector. For example, Finland boasts roughly 4,988,000 cellular phone users, as well as, 3,286,000 internet users. There are many programs and strategies applied in Finland to enhance the information sector. For example, the Government Information Society Programme is one of the most common programs used into Finnish market. This programme consists of two aspects: broadband strategy and the information security strategy. These strategies underline the importance of information security and point out that information security is not only technical issue but also more and more of an economic and social issue ([www.e.finland.fi](http://www.e.finland.fi)).

Moreover, the Finnish society has a National Information Security Day which aims at increasing Finn's awareness of the risks of the internet and provides information and advice on how to protect oneself against information security threats ([www.tietoyhteiskuntaohjelma.fi](http://www.tietoyhteiskuntaohjelma.fi)).

In Finland there is a Finnish Communications Regulatory Authority (FICORA) which is responsible for enforcing information security policies in telecommunications companies, protect privacy in electronic communications, and prevent and resolve information security breaches as well as aims to promote information security and privacy protection in communications networks and services ([www.ficora.fi](http://www.ficora.fi)).

### 3.2.2 Jordan

Jordan is one of Arab countries which is located in Middle East, with a population of 5.906 million for (2006), and population growth rate of 2.49%. Labor force in Jordan was 1.460 million during 2005. GDP per capita was \$4.800 with growth rate of 5.9%. 91% of Jordanians are literate ([www.cia.gov](http://www.cia.gov)). The education system in Jordan has been ranked to be thirteenth in the world regarding meeting the needs of a competitive economy (IMD, the world Competitiveness Yearbook 2005).

Structure of Jordanian organizations has changed over last decade. The volume of exports was \$4.226 billions (2005). Most popular exports commodities in Jordan are: phosphate, cement, potash, and light manufacturing. The volume of imports was \$8.681 billions (2005). Most popular imports commodities in Jordan are: crude oil, machinery, transport equipment, and food ([www.cia.gov](http://www.cia.gov)).

There has been a remarkable progress in IT sector during last decade in Jordan. Most of this progress was done in a personal uncoordinated manner. Short of cooperation and coordination procedures had contributed to the emergence of incompatible IT infrastructure. In spite of the wide spread recognition of the importance of information, information systems, and uses of information services are still quite traditional. In mid-2000, the Government of Jordan announced that strengthening the IT sector was a national priority. A national strategy for IT development, known as the REACH Initiative, was developed by Jordanian public and private sector entities.

The overall goals of the initiative included developing an internationally competitive IT industry that will attract international and local investment, generate high-value jobs and produce substantial levels intellectual capital ([www.intaj.net](http://www.intaj.net)).

According to CIA fact book, Jordan has around 600,000 internet users and 1,594,500 cellular phone users until 2005. Since, software and IT sectors comprise one of the most dynamic and fastest-growing sectors of globe economy; therefore there are many reasons that induce private and public sector in Jordan to enlarge their focus on these sectors. Some of the reasons are listed below:

- Low start-up capital requirements
- Jordan's favorable position in the regional market
- Human resource intensity
- Not affected by distance or transportation constrains

**Table 3- 1** Economical and Technological indicators of studied countries

<b>Indicator</b>	<b>Finland</b>	<b>Jordan</b>
Population	5.231 Million (2006)	5.906 Million (2006)
Growth rate of population	.14%	2.49%
Literacy of population	100%	91%
Rank of the educational system, in the world, to meet the needs of a competitive economy	First	Thirteen
Internet users	3,286,000	600,000
Internet hosts	1,503,976	3,160
Cellular phone users	4,988,000	1,594,500
Labor force	2,61 Million	1,46 Million
GDP per capita	\$30,600 (2005)	\$4,800 (2005)
GDP Growth rate	2.2% (2005 est.)	5.9% (2005 est.)
Volume of Exports	\$67.88 billion (2005)	\$4.226 billion (2005)
Volume of imports	\$56.45 billion (2005)	\$8.681 billion (2005)

Subsequently, I would analyze and conclude situation of studied countries towards managing information security. The previous table consists of all important indicators related to economic and IT situation in both countries.

Finnish companies are more developed than Jordanian companies for many reasons. **Economic indicators:** Labor force in Finland is 2.61 million with \$30,600 as GDP per capita, whilst labor force in Jordan is 1.46 million with \$4,800 as GPD per capita. Volume of exports in Finland is 67.88 billion dollars and 4.226 billion dollars in Jordan. Volume of imports in Finland is 56.45 billion dollars and 8.681 billion dollars in Jordan. Based on previous comparative indicators, Finnish economy seems to be stronger than Jordanian economy. Since, the Finnish economy is stronger; companies in Finland are larger and developed than Jordanian companies. The international success of Nokia and many smaller companies has been seen as a proof of the competitiveness and strengthen of the Finnish economy.

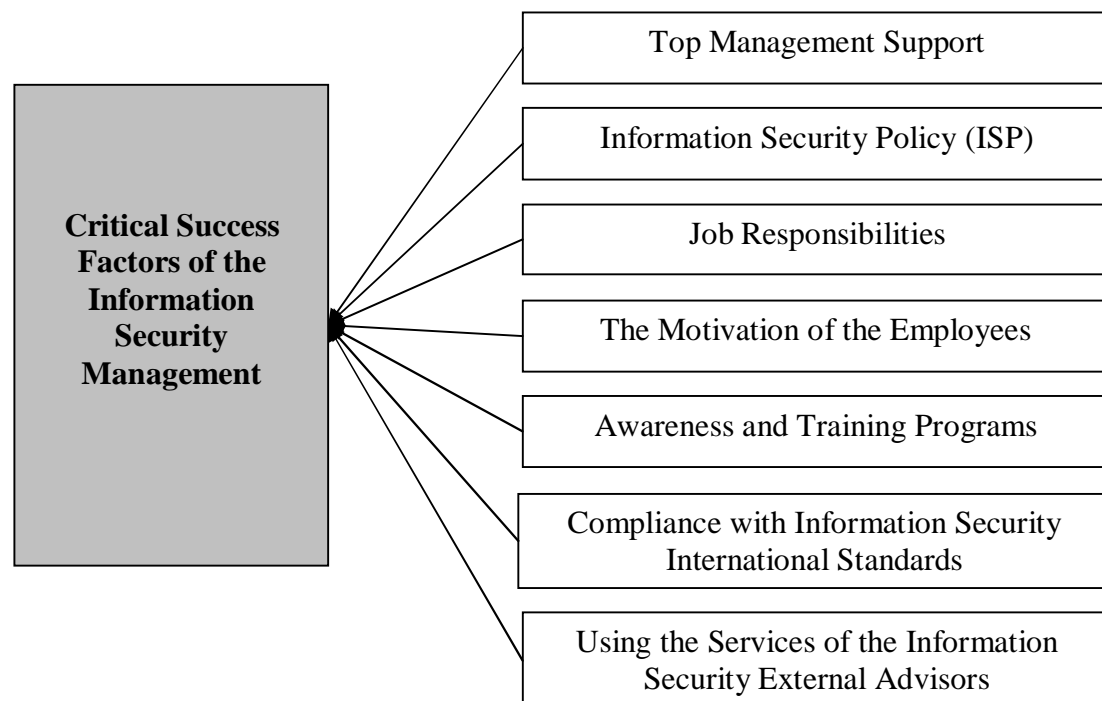
**Education indicators:** Finland and Jordan have roughly the same number of population. 100% of Finns and 91% of Jordanians are literate. Finnish education system has occupied the first rank in the world towards meeting the needs of competitive economy, whilst Jordanian education system occupied rank thirteen. **Technological indicators:** Finland has 3,286,000 internet users with 1,503,976 internet hosts, as well as, 4,988,000 cellular phone users. Jordan has 600,000 internet users with 3,160 internet hosts, as well as, more than 1.5 million cellular phone users. These significant differences between Finland and Jordan in technology sector show that Finnish IT sector is advanced and developed than Jordanian IT sector.

**Organizational indicators:** Several programs and strategies are applied in Finland and Jordan to protect information assets and develop the IT sector. For example, in Finland there is the government information society program, and National Information security day. Both of these programs aim at enhancing awareness of information security among Finnish companies. Finnish communication Regulatory Authority has been founded to organize information security issues in telecommunications sector. In Jordan, a notional strategy for IT sector development known as the REACH initiative that developed by Jordanian public and private sector

entities. REACH initiative aims at developing an internationally competitive IT industry to attract international and local investments, and generate high-value of jobs opportunities.

### 3.2 Success Factors of Information Security Management

The following model shows the success factors associated with ISM. Testing factors will be incorporated in the empirical research chapter.



**Figure 3- 1** *Success factors of Information Security Management (ISM).*

#### 3.2.1 Top management support

One of the most important issues, for all the interested parties in an information security, is to get sufficient support from the top management. If the top managements of organizations are aware of the importance of keeping information assets safe, they are most likely to support and encourage the activities of ISM. Most probably the support received from top management results into availability of financial and technical resources (Kankanhalli et.al 2003).

Kankanhalli et.al (2003) mentioned that organizations with less top management support are likely to invest less in ISM. This would lead the organizations to serious information security problems. It is better for such organizations to enhance the interest of ISM

Deficient support received from the top management for managing information security has been recorded as one of the biggest drawbacks to have an effective ISM in most of the organizations (Solms R. 1996). Objectives of managements are to have high share of market, increase product quality and other strategic objectives. However, importance of information security becomes one of the most priority advantages to have new clients and expanding through the market. While careless of information security will lead for lose in market shares, decrease potential clients etc. Thus, top management should not separate between achieve its objectives and keep their information assts secure.

The board of directors and top management has a direct corporate governance responsibility towards ensuring that all the information assets in the organization are adequately secure (Solms & Solms 2004). Therefore, they should pay high attention to maintain and protect information assets against misuse or loss. Hone & Eloff (2002) mentioned that the management commitment towards information security is considered as an absolutely essential factor in ISM. Without commitment of the management, any activity attempted to improve ISM will not be taken seriously through the entire organization.

The support and commitment of the top management to understand the information security problem were observed as one of the most important factors for an efficient of ISM implementation. Bjorck (2001) had developed empirical study on Swedish data and documented that overwhelmingly most of the respondents considered support received from top management as the most important factor in ISM.

### 3.2.2 Information security policy (ISP)

Corporate ISP is the heart of any successful ISM. Any information security plan, no matter how well designed and implemented, will has to have the ISP. The fact that

ISP plays a crucial role in managing information security makes it the most crucial document for ISM (Solms & Solms 2004).

ISP is the main instrument used by ISM to demonstrate the need for and scope of information security. ISP used to document the management commitment towards information security, maintaining the continuity of operations, ensures continuity of services providing, and protecting the information asset harmonically (Nosworthy J. 2000; Siponen M. 2005). Since ISP is a main tool used in ISM plan, it is very important to know what ISP incorporates.

There are many methods used to document and develop an efficient ISP. One of the most common methods are often used by many organizations is to have a look on other developed policies and adapt them according to their needs. However, the created policies based on this method will truly not reflect the culture, objectives and management commitment of the organization. Therefore, there are some points must be taken into account during the policies development process. Hone & Eloff (2002) identified that some additional points based on organizations requirements should be taken into account while developing ISPs. It is very important to have an adequate support from the end-users as they must have full understanding regarding protection of information security issues. If ISP does not reflect organization's culture, objectives and management commitment, it will not have a sufficient support from end-users.

There are elements that should be available in ISP in order to achieve its objectives coherently with organization's objectives. Some of them are as follows (Hone & Eloff, 2002; Karyda et.al 2004).

1. Need for and scope of information security,
2. Objectives of information security
3. Definition of the information security
4. Management commitment to information security
5. Approval of the information security policy (signature)
6. Purpose or objectives of the information security policy
7. Information security principles

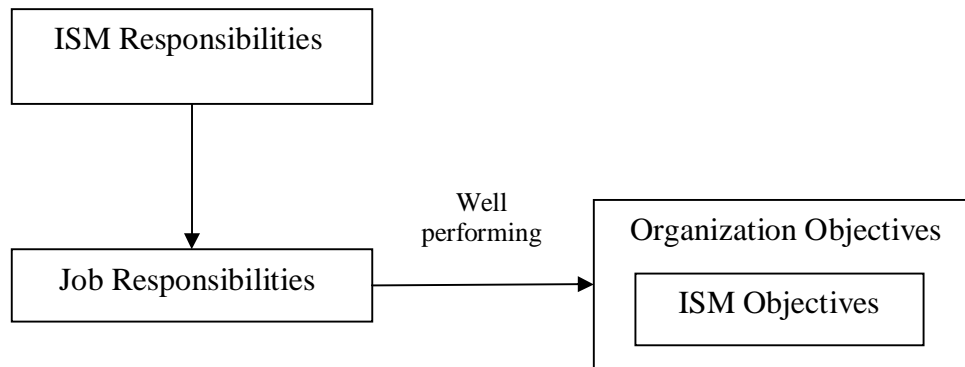
8. Roles and responsibilities
9. Information security policy Violations and Disciplinary Action
10. Monitoring and Review
11. User declaration and acknowledgement

### 3.2.3 Job Responsibilities

Job Responsibilities are structured in a reasonable way to make the organizations able to perform its functions successfully (Toval et.al 2002 pp 205-219). Coherently, allocating the information security responsibilities amongst the employees has been integral to ISM success. Thus, structuring of the job responsibilities such that they define and clarify information security tasks for every employee are considered as defining factors in ISM success (Bjorck F. 2001).

Defining information security responsibilities designate information ownership to employees and thus enable employees to perform their duties towards information security efficiently. Therefore, the employees should be responsible for information security requirements throughout the lifecycle of information process from initiation to dumping (Nosworthy J. 2000). The ISP has been found to comprise all information security responsibilities that enable the employees to know what is exactly expected from them to do in term of protecting information assets (Hone & Eloff 2002).

The following figure shows how the job responsibilities and ISM interact together to have a secure information environment and achieve the objectives of the organization coherently. Managing information security plays an important role to configure some parts of job responsibilities in order to secure the information assets. Well performing of these responsibilities will coherently achieve the goals of organization and ISM. The importance of the job responsibilities come up through defining the activities of ISM for every employee.



**Figure 3- 2** *ISM and Job Responsibilities*

### 3.2.4 Motivation of Employees

Many articles have discussed the role of the human factor in ISM. Some of these articles have mentioned the importance of this factor from several perspectives such as risk management, mistakes, abuses, and other threats that might be caused by humans (Solms & Solms 2004; Gonzales & Sawicka 2002; Gary H. 2003). Managing information security should seriously consider the role of motivation of employees, because deploying more procedures and controls is not sufficient to engage the employees in the information security process. Instead, employees should be convinced and encouraged to perform their information security duties successfully.

Motivation of employees has an important role for success of ISM, where information security managers and those responsible for different areas in organization should be motivated in order to exploit information security activities successfully. (Bjorck F. 2001). The involvement of employees to protect information asset will enhance as the understanding towards ISM benefits increase (Kankanhalli et.al 2003).

Nosworthy (2000) pointed out that employees should be motivated enough towards adopting the ISM activities in order to make them successful. Therefore, I expect this factor to be integral to ISM success. Employees, being responsible for executing policies and operations in any organization, are thus important for the success of ISM to be successful.

### 3.2.5 Awareness and Training programs

Lack of awareness and understanding of information security is one of the most important factors that prevent any attempt to effectively communicate and implement the ISM activities. Since, the information security is an intangible issue; it is very difficult for organization to realize the importance of this issue without running and implementing awareness and training programs (Mitchell et.al 1999). The aim of awareness and training programs is to enable employees to realize the fact that information security is a business issue rather than technical issue. Regrettably, a lot of organizations still have the mind set that information security is a technical issue therefore all the information security issues posted to IT department (Solms & Solms 2004).

If the users are unaware about risk associated with using information assets, the potential damage caused by users could be unpredictable and the users would not be held responsibilities (Solms & Solms 2004). Involvement of employees in information security has several perspectives. On one hand employees tend to be disloyal as they are attempted to steal or copy information that seem profitable to them (one of the main reasons for unauthorized access to confidential information). On the other hand, employees are poorly trained in terms of security or unaware of how to operate the computing machines, therefore mistakes of those users will arise as they do not really know what they are doing (Lau O. 1998).

Understanding the importance of security awareness and training programs is formulated as one of the main requirements of ISP (Nosworthy J. 2000). Running the awareness and training programs has gained several important benefits such as

- Providing a flexible communication forum that enables the staff to tell if they don't understand,
- Raises awareness and importance of information security issue through using continuous awareness and training programs in order to encourage users and make them more interested to learn as much more as about information security.
- Changing user attitudes, by making them learn how to view things more objectively.

- Enables ownership: It will allow staff to understand their responsibilities more and allow them to take an ownership for their part of the implementation of the ISM plan
- Sustaining the continuity of operations ensures that all the staff is equipped with sufficient knowledge, thereby enabling an effective ISM implementation.
- Giving third parties more satisfaction: If the third parties can observe that the organization is committed to investing in the needs of people then in turn they will get more efficient.

Therefore I expect that awareness and training programs are playing a crucial role in achieving and supporting the ISM activities. Since, we can not involve employees in information security unless they do not know what to do toward information protection therefore; importance of awareness and training programs is integral to ISM success.

### 3.2.6 Compliance with information security international standards

Compliance with information security international standards will positively enhance the external parties' expectations, especially when organizations declare that they are adopting information security international standards (Eloff & Eloff 2003). Most of these standards are developed based on personal observations. Therefore, a full compliance with international standards may be 'a bridge too far' for many companies and inappropriate for them. This means that when organizations attempt to use these standards they could not consciously consider the organization culture, and other related issues which may make the ISM plan fuzzy and less understandable by the end-users even the high level of managers. Some of the information security international standards are described in the following table;

**Table 3- 2** Information security standards

<b>Standard</b>	<b>Description</b>
BS 7799	They are UK standards that cover the management of information security. Part 1 of the BS 7799 consists of Code of practices for information security management, as well as there is another exclusively part for review and evaluation the information security policy ( <a href="http://www.bsi-global.com">www.bsi-global.com</a> ).
COBIT	Control Objectives for Information and related Technology (COBIT) has been developed by the Information Systems Audit and Control Association & Foundation (ISACAF). The aim of COBIT is to provide management and business owners with an IT governance model to help them understand and manage the risk associated with IT ( <a href="http://www.isaca.org">www.isaca.org</a> ).
GASSP	General Accepted Systems Security Principles (GASSP) are published by United States of America's National Research Council in 1990. They are basically a set of general accepted system security principles developed based on recommendations of a report Computer At Risk ( <a href="http://www.theiia.org">www.theiia.org</a> ).
GMITS	The main purpose of GMITS, Guidelines for the Management of IT Security, is to provide a comprehensive guidance for planning, managing and implementing of the information security plans ( <a href="http://www.bsi-global.com">www.bsi-global.com</a> ).

Feasibility, the organizations will save some money and efforts by adopting these international standards because they do not need reinvent the regulations and procedures that were already sited by the international standards (Hone & Eloff 2002). The compliance with these standards provides a common basis for all companies to develop, implement and measure the effective security practices, and used them to enhance the confidence amongst organizations (Solms R. 1999).

### 3.2.7 Using services of information security external advisors

The shortage of information security experience and practices inside organization has induced most of the organizations to rely on external parties to manage their information security. Access to those information security experts is crucial factor to have enough support for managing information security (Bjorck F. 2001). The need for external competences depends on the organizations requirements in regard of

information security. There might be some organizations that do not have sufficient qualified staff so they have to rely on external advisors for ISM.

Recruiting new information security advisors is quite hard and critical. Usually, the HR department co-ordinates with IT department to perform this mission but this mission is still not easy for many organizations. Therefore, these organizations tend to rely on outsourcing recruitment agencies to hire a qualified advisor complies with their requirements (Nosworthy J. 2000).

The need for external experts and advisor has some benefits; it would be useful for organizations to contact external experts as they might enhance the knowledge of their internal staff and minimize relying on information security external specialists in future (Finne T. 1998 pp 80-83).

### 3.3 Summary and conclusion of chapter

Research model of my study consists of two main parts. First part discussed the market situation of studied countries. This section has shown that both countries differ at level of economic and technological progress. Based on indicators in table 3-1, Finnish market is technologically and economically larger and stronger than Jordanian market.

Second part was discussed success factors of ISM. ISM should conduct all the security requirements to offer an adequate protection for information asset against any loss or misuse. All of the seven mentioned factors play an important role in success of ISM. Figure 3-1 shows the research model with these factors. As summarized below and discussed in previous theoretical and empirical literature, these factors play an integral role in success of ISM.

- § Top management support is essential as it provides sufficient moral and financial support for ISM.
- § Information Security policy is important as it is a main instrument for achieving the activities of ISM.

- § Job Responsibilities demonstrate and clarify the responsibility of every employee towards managing information security. Therefore, making it essential for the success of ISM.
- § Motivation of employees enhances the success of ISM through convincing the employees about its objectives and benefits.
- § Awareness and training programs play an important role to increase the consciousness of the employees and those are essential for the success of ISM.
- § Compliance with information security international standards offers general accepted roles that allow the organizations to assess their security level as well as the security situation of other organizations and to make decision in order to share their systems together.
- § Finally using services of information security external advisors allows ISM actors share information security knowledge.

## 4. Research Methodology

### 4.1 Objectives and structure of the chapter

Aim of this chapter is to introduce the research hypotheses and describe data gathering process, as well as analyze total of received responses.

The structure of the chapter is as follows;

Section-1: Objective of chapter

Section-2: Research Hypotheses

Section-3: Data Gathering and Descriptions of targeted sample and survey method

Section-4: Total of Received Responses

### 4.2 Research Hypotheses

This section consists of two parts. First part investigates if there is a significant difference between Jordanian and Finnish respondent companies towards the importance of factors discussed in previous chapter. Second part discusses the importance of the success factors for managing information security.

#### 4.2.1 Top management support

Few studies have discussed the influence of the top management support as a success factor for managing information security. These studies document that the commitment and support received from the top management is an important factor for managing information security successfully. Top management's support has been found to be responsible for initiating awareness and training programs, committing to the Information Security Policy (ISP), and allocating more resources to improvement of information security environment.

*H1.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of top management support for the success of ISM.*

*H1.2: Top management support is important factor for the success of ISM.*

#### **4.2.2 Information Security Policy (ISP)**

ISP is the main instrument used by ISM to demonstrate the need for and scope of information security. Practically, ISP expresses top management's commitment towards protecting the information assets. There are many international standards that explain the procedures and controls that should be conducted into ISP. Adopting these international standards gives ISP an integral role in the success of ISM. Many theoretical studies have documented the importance of ISP.

*H2.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of ISP for the success of ISM.*

*H2.2: ISP is an important factor for the success of ISM.*

#### **4.2.3 Job Responsibilities**

Job responsibilities play an important role in clarifying and defining how the responsibilities of information security will perform inside of the organization. However, allocating these responsibilities amongst employees has an important role to play in supporting the activities of ISM. Few previous studies have declared job responsibilities as an important factor for the success of ISM.

*H3.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of job responsibilities for the success of ISM.*

*H3.2: Job responsibilities are important factor for the success of ISM.*

#### **4.2.4 Motivation of Employees**

Information security participants, managers, and those responsible for different areas in the organization should be motivated to securely exploit the information security activities. Several studies have focused on the human factors and how these factors should be managed for successful implementation of ISM plan. The importance of the motivation is to make the employees highly convinced about the benefits of information security efforts.

*H4.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of motivation of employees for the success of ISM.*

*H4.2: Motivation of employees is important factor for the success of ISM.*

#### **4.2.5 Awareness and Training programs**

Awareness and training programs enable the organization's employees to understand information security aspects and convince them about the fact that information security is a business issue rather than a technical issue. Unfortunately, a lot of organizations still think that the technical solution is all that is required to solve information security issues.

*H5.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of awareness and training programs for the success of ISM.*

*H5.2: Awareness and training programs are important factor for the success of ISM*

#### **4.2.6 Compliance with Information Security International Standards**

The importance of these standards comes through enhancing the confidence amongst the organizations. Adopting international standards provides organizations with an adequate assurance to safely interact with each others. Implementing these standards will significantly effect on ISM and achieve organization's objectives coherently.

*H6.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of compliance with information security international standards for the success of ISM.*

*H6.2: Compliance with the information security international standards is important factor for the success of ISM.*

#### **4.2.7 Using Services of Information Security External Advisors**

Some of the organizations are suffering of insufficient experience in the information security issues. Therefore, these organizations have induced to relay on information security external advisors to support their ISM activities. In addition, some of these organizations are unable to specify what are the requirements that should be available in the advisors or experts that they are looking for. Therefore, they rely on recruitment agencies to find out such external experts.

*H7.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of using services of information security external advisors the success of ISM.*

*H7.2: Using service of information security external advisors is important factor for the success of ISM.*

## 4.3 Data Gathering

### 4.3.1 Sample description

The survey aims to find out how the Jordanian and Finnish companies manage information security. Recently, most of the organizations are realizing the paybacks of keeping their information environment safely. Thus my intention is to pay attention on finding out the perspectives of the companies regarding the importance of success factors surrounding of ISM. Prior literature documents the importance of these factors in the success of ISM. However, investigating these factors in the context of Jordan and Finland that are at different level of economic and technology development make my study interesting.

Research survey has targeted medium and large sized companies located in Finland and Jordan. The sample was selected based on companies' annual turnover of 20 million dollars for Finnish companies and 10 million dollars for Jordanian companies. Information contacts of the Jordanian targeted companies were extracted from the INTAJ Database. The Intaj database is one of publicly accessible databases that provide business contact information for Jordanian companies. The information contacts of the Finnish targeted companies were extracted from the Blue Book's company database. Blue Book is a provider of business contact and marketing information of the Finnish companies.

Online survey was e-mailed to 180 Finnish companies and 85 Jordanian companies. Focused of the survey was to email questionnaire to certain titles such as Chief Information Officers (CIO) and the Internal Auditing Department heads.

### 4.3.2 Survey Description

The internet-based survey software which is provided by Webropol Oy was used to develop the online survey for this study. Webropol Oy is one of the market leaders in Finland for producing internet-based survey software (Webropol RTA). They have over 500 customers in Finland. The Swedish School of Economic and Business Administration (Hanken) is also one of the Webropol Oy's costumers. I have been established the database of the survey by coordinating with Data department in Hanken. By coordinating with Hanken's data department, the reliability of online research survey has been enforced.

The survey was established in two separate databases to distinguish between respondents of each country. Copy of online survey was e-mailed to Jordanian targeted companies and another copy of the same survey was e-mailed to Finnish targeted companies. The received responses of each targeted sample have submitted into separate databases which make the comparative analysis process more efficient and informative

The survey was divided into two main parts. Four questions were asked into the first part that investigates the background information of the respondent companies. The first question investigates number of employees. Second question investigates availability of separate department for ISM. The third question compliments the second question by asking if there is any separate department for managing information security. Respondents were asked to define what other department was tackling ISM activities. The forth question investigates the years of experience of the respondents.

Second part of survey was used to measure and investigate the opinion of respondents towards importance of factors associated with ISM. This part of the survey consists of seven sections; one section per factor of the research model. Each section consists of three questions. One of them is a main question and the other two questions enforce the answer of the main question. For example, top management support section contains three questions. One of them is the main question that measures the importance of this factor as success factor for managing the information security. The other two questions are developed in context of enforcing and supporting the answer

of this question. The two questions are: is managing information security part of overall corporate strategy of respondent company? How often are top managements of respondent companies involved in reviewing and approving the ISM plans?

Several types of questions were adopted to give respondents more flexibility to express their perspectives towards these factors. For example, one type of questions were scaled from 1 to 4 to measure the importance of the success factors, and other type of questions represented by Yes and No that are used to investigate the availability of some factors, e.g. availability of ISP.

Enhancing the secure relevance, validity and reliability of this survey was achieved by several-round process of revisions. I evaluated all of the questions carefully in consultation with my supervisor Mr. Anders Tallberg. The survey was, then, sent to a panel of PhD students for further review. At the end, the survey got the approval from Mr. Anders Tallberg after his last review and evaluation.

#### 4.3.3 Survey questions and used for testing Hypotheses

Testing hypotheses was done based on specific questions presented in the survey. The following table shows the survey questions used for testing hypotheses.

**Table 4- 1** Survey questions used for hypotheses

<b>Factor</b>	<b>Hypothesis</b>	<b>Survey Question</b>
Top Management Support	H 1.1	How important is the support received from Top Management in the success of managing the Information Security?
	H 1.2	
Information Security Policy	H 2.1	How important is the information security policy in managing the Information security in your organization?
	H 2.2	
Job Responsibilities	H 3.1	How important are the Job Responsibilities in the success of managing the Information Security?
	H 3.2	
The Motivation of the Employees	H 4.1	Is defining the information security responsibilities in advance for each job important for success of managing the Information security?
	H 4.2	
Awareness and Training Programs	H 5.1	How important are Awareness and Training Programs for the successful management Information Security?
	H 5.2	

Compliance with Information Security International Standards and guidelines	H 6.1	How important is the compliance with International Standards of Information Security for the overall success of Information Security Management within your organization?
	H 6.2	
Using Services of Information Security External Advisors	H 7.1	Do you believe the use of consultants and external advisors plays a part in the success of managing your organizations information security?
	H 7.2	

#### 4.4 Total of Received Responses

Thirty responses were received from Finnish companies and twenty eight responses were received from Jordanian companies. The survey was e-mailed during the period "between" 02-06 to 02-20-2006. The survey was e-mailed to 180 companies in Finland. Out of these 180 emails, 28 e-mails not delivered to final respondents. Therefore, I left them out of Finnish targeted observations. The total of the Finnish targeted companies is 152 companies instead of 180 companies. The same survey was e-mailed for 85 of the Jordanian companies. After two weeks of e-mailing the online survey and performing a three rounds of reminding the targeted employees; the responses rates were 33% Jordanian observations and 20% for Finnish observations.

**Table 4- 2** Data Gathering results

	Finland	Jordan
Targeted companies	152	85
Received responses	30	28
Percentage of Responses	20%	33%

## 5. Empirical Results

### 5.1 Objectives structure of the chapter

This chapter aims to analyze and describe the collected data, as well as test the hypotheses of the research model.

Section-1: Analysing methods, analysing the survey responses, and analysing the background information of the respondent companies.

Section-2: Description of the collected data and testing first part of the Hypotheses (Comparative analysis between Jordanian and Finnish observations).

Section-3: Testing the Second part of the Hypotheses (important of these success factors for managing the information security).

### 5.2 Analysing method

The analysis was done with statistical package, SPSS. I used parametric and non-parametric statistical techniques to test my hypotheses. Parametric techniques used for testing continuous variables such as years of experiences, while non-parametric techniques are ideal for testing nominal and ordinal data. With the help of these statistical techniques, I measured the validity of theoretical model and hypothesis.

Chi-Square Test is a non-parametric test which is used to determine whether two categorical variables are related. It compares the frequency of cases found in the various categories of one variable across the different categories of another variable. One of the general assumptions of chi-square test is that the minimum frequency for each cell should not be less than 5. Therefore, all of the cells that have frequency less than 5 were merged with other related cells in order to run the chi-square test. Continuity correction was used to measure the significant relationship for tables that consist of 2x2 matrices, while Pearson chi-square was used to measure the significant relationship for matrices more than 2x2.

If the P-value of Pearson Chi-Square or continuity correction is less than .05, I conclude that statistically strong relationship between variables is present. P-value

between .05 and .10 refers to weakly significant relationship between variables, while p-value greater than 0.10 refers to insignificant relationship.

Cross tabulation shows the percentages of respondent for each variables when they answer the targeted question. I described how to read these tables in section 5.4.1 for the variable "top management support", while tables for other variables have been posted in the Appendixes B and C.

## 5.3 Respondent Companies Background Information

### 5.3.1 Number of Employees

This is the first part of the collected data and investigates the background information of the respondent companies. Since, ISM activities are more informative to measure by number of employees, therefore first question of the survey deals with number of employees of the respondent companies. Following table illustrates distribution of the number of employees amongst the Jordanian and Finnish samples.

**Table 5- 1** Number of the employees of respondent companies

Number of Employees	Finland		Jordan	
Less than 500	12	40%	14	50%
501 - 2000	11	36%	12	42.8%
2001 - 5000	2	6.6%	2	7.2%
More than 5000	5	16.6%	0	-
<b>Total of responses</b>	<b>30</b>	<b>100%</b>	<b>28</b>	<b>100%</b>

It seems that most of the respondent companies are working with quite a large number of the employees. In Jordan, 50% of the respondent companies (14 companies) are operating with less than 500 employees, 42.8% (12 companies) are working with 501-2000 employees, and 7.2% (2 companies) with 2001-5000 employees. On the other hand, Finnish respondent companies show that 40% (12 companies) are operating with less than 500 employees, 36% (11 companies) with 501-2000 employees, and 6.6% (2 companies) with 2001-5000 employees. Finally there are 16.6% (5

companies) companies in Finland that have more than 5000 employees. Most of economical and technological indicators presented in table 4-1 show that the organizations in Finland are larger than the organizations in Jordan. For example; in Finland total exports are \$67.88 billion and total imports are \$56.45 billion. Whilst in Jordan only total exports and imports are \$4.226 billions and \$8.681billions respectively. Finland has 3,286,000 internet users with 1,503,976 internet hosts, as well as, 4,988,000 cellular phone users. Jordan has 600,000 internet users with 3,160 internet hosts, as well as, more than 1.5 million cellular phone users.

As can be seen from table 5-1, most of respondent companies have a large number of employees. As I have mentioned earlier; number of employees plays crucial role in quality of managing information security, therefore organizations with large number of employees would consider managing information security seriously more than companies with little number of employees.

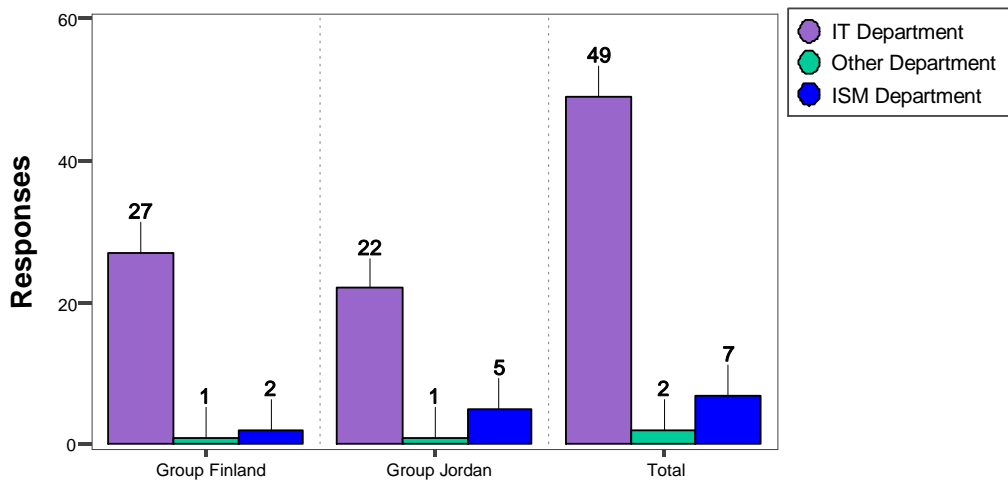
### 5.3.2 Independent Department of Information Security Management

*1- Does your organization have a separate Information Security Management (ISM) Department?*

*2- Which department manages Information Security Management (ISM) issues?*

Previous two questions ask whether the respondent companies have a separate ISM department or not. In case, there is no a separate ISM department, which other department is taking care of this mission? Following figure shows the distribution of respondent companies that have or have not ISM department. The x axis represents the group of countries and the departments that manage information security. The y axis shows number of the respondents.

### The Department Suppose to Manage the Information Security



**Figure 5- 1** Information Security Management Department

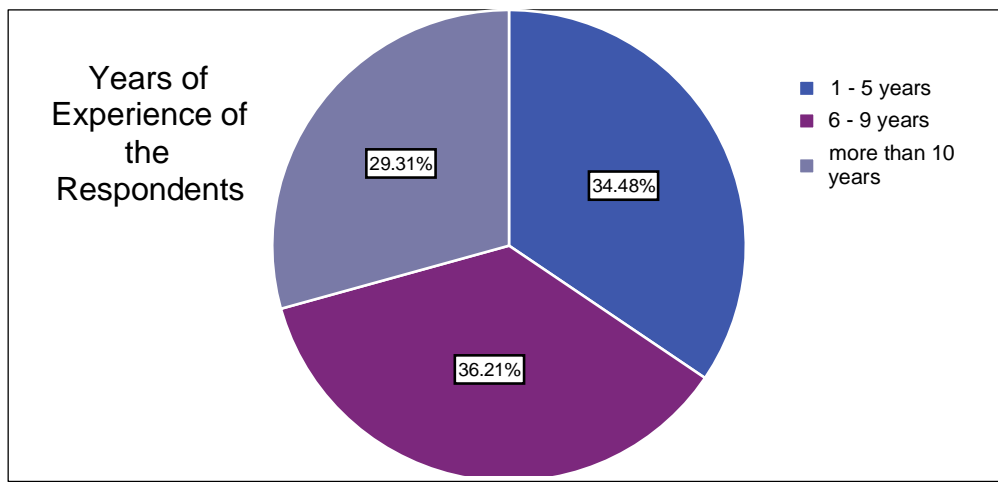
As shown in the figure above, 84.48% of the respondents (49 companies) are posting ISM activities for IT department. High percentage of these respondents believes that managing information security is the responsibility of IT department. 12.07% (7 companies) have a separate ISM department. I expect they are realizing the importance of having a separate department for ISM instead posting these responsibilities to IT and other departments. 3.45% of the respondents (two responses) posted ISM activities to Human resource department and the other one to financial department. Those two respondent companies have quite small number of the employees, and they may have no IT department at their companies so they have allocated these information security activities to other departments.

### 5.3.3 Years of Experience of the Respondents

Experience of respondents enhances the validity and reliability of responses. Therefore, this question has been developed to check whether the respondents have sufficient years of experience in information security assignments or not. It seems most of the respondents have many years of experience in information security. The following figure shows distribution the years of the experience for all the respondents.

These years are classified into three scales 1-5 years, 6-9 years, and more than 10 years.

As presented in the following figure, 34.48% (20 respondents) have years of experiences less than 5 years. 36.21% (21 respondents) have years of experience between 6 – 9 years, and 29.31% (17 respondents) have years of experience more than 10 years



**Figure 5- 2** *Years of Experience of the Respondents*

It is informative to investigate if *there is a significant difference between Jordanian and Finnish respondent in regard of years of experience*. I have got the following results after running the T-Test.

**Table 5- 2** *T-Test Statistics of Years of Experiences*

T-Test Statistics				
Group	N	Mean	Std. Deviation	Std. Error Mean
Finland	30	8,13	3,421	,625
Jordan	28	6,54	2,531	,478

**Table 5- 3 Independent Sample Test of Years of Experience**

Independent Samples Test									
	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
								Lower	Upper
Equal variances assumed	1,901	,173	2,010	56	,049	1,598	,795	,005	3,190
Equal variances not assumed			2,031	53,30	,047	1,598	,787	,020	3,175

As can be noticed from the above tables, the Significant (2-tailed) value is .047. This concludes that there is a *significant difference* between the observations. This means that the proportion of years of experience for the Jordanian respondents is significantly different from the proportion of the years experience for the Finnish respondents. Table 5-2 shows the average of years of experience is 6.54 for Jordan and 8.13 for Finland. This means that Finnish respondents have years of experiences significantly more than Jordanian respondents. Since Finland a developed country it would be normal to have employees with high years of experience. Although, Jordan is a developing country but it seems that the Jordanian companies are interested to have employees with good experience of managing information security.

## 5.4 Description of Data, Testing Hypotheses of the Comparative Analysis

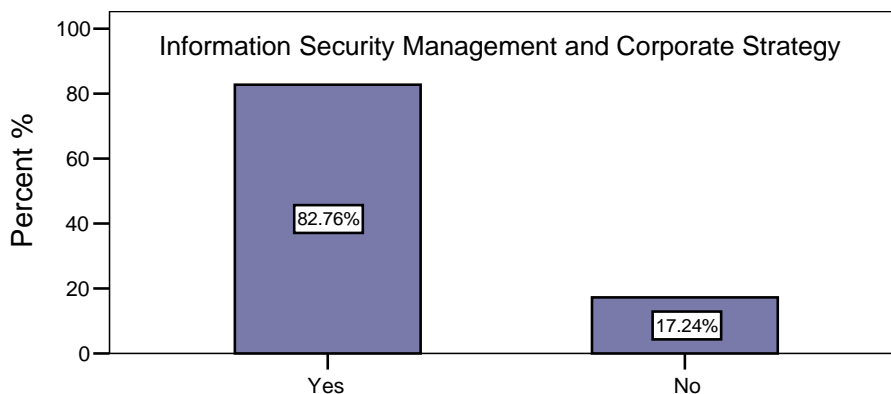
Aim of this subsection is to describe the collected data and testing the first part of the hypotheses (comparative analysis).

### 5.4.1 Top Management Support

This section shows the perspectives of respondents towards the importance of Top Management Support as a success factor managing information security. This section

spells three questions. First question explores whether managing information security is part of overall corporate strategies of the respondents companies. Second question shows the frequency of involvement of top management in reviewing and approving the ISM plans. Third question obviously investigates importance of this factor. This question will be used for comparative analysis between Jordanian and Finnish observations.

**First Question: Is managing information security in your organization part of overall corporate strategy?** This question investigates whether managing the information security is a part of overall corporate strategy of the respondent companies or not. Following figure shows that if ISM is integral part of corporate strategy. The x axis represents the respondent companies who are/ aren't considering of managing information security into their overall corporate strategies. The y axis represents the percentage of respondents.



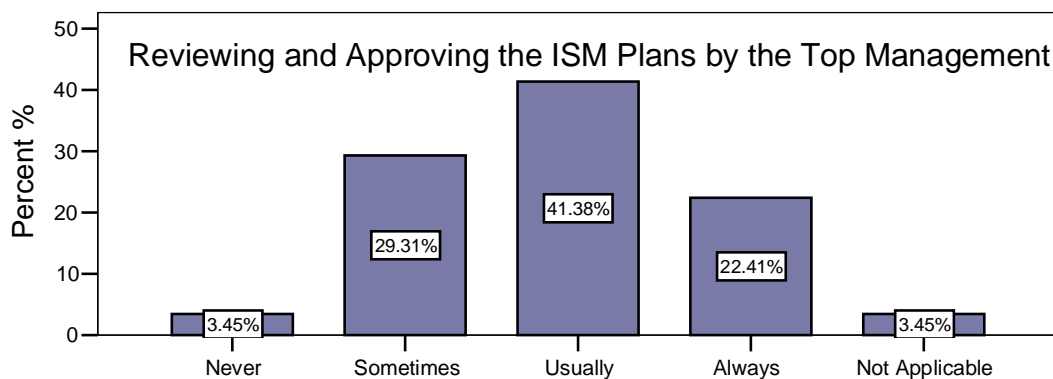
**Figure 5- 3** *ISM and Corporate Strategies*

The above figure shows 82.76% of the respondents (48 companies) have declared that their organizations consider information security management into their overall corporate strategy, and 17.24% of the respondents (9 companies) are not considering the managing information security into their corporate strategies. It seems that high percentage of companies are considering the ISM into overall their corporate strategies because they may realize the importance of managing information security, as well as the risk that could arise if they are not considering in managing information security.

Within the companies that consider ISM as integral part of their corporate strategy, 85.7% acknowledged Top Management Support as an important factor for ISM success. Within the companies that do not consider ISM as integral part of their corporate strategy, 14.3% acknowledged Top Management Support as an important factor for ISM success (see table 5-22, appendix C). Even the respondent companies who do not consider ISM plan into their corporate strategy approve that this factor is important for managing information security successfully.

**Second Question: How often is top management involved in reviewing and, subsequently, approving the Information Security Management (ISM) plans?**

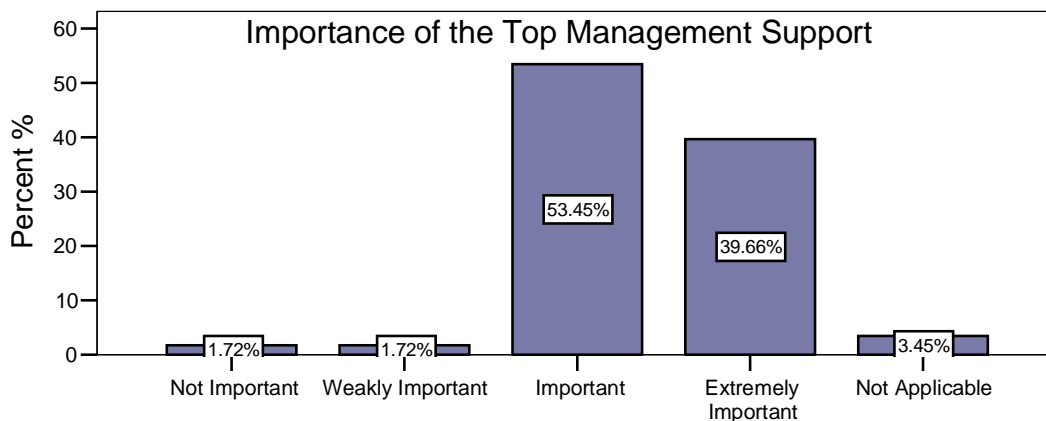
This question inquires the involvement of the top management in reviewing and, subsequently, approving ISM activities. The next figure shows the frequency of reviewing and approving ISM plans by top management. The x axis represents the frequency of reviewing and approving ISM plans. The y axis represents the percentage of respondents.



**Figure 5- 4** *Reviewing and approving the ISM plans by the top management*

As displayed by the above figure, 41.38% (24 respondents) have indicated that their top managements are USUALLY reviewing and approving ISM plans. 22.41% (13 respondents) have referred that their top management are ALWAYS doing these reviewing and approving processes. Whilst 29.31% (17 respondents) have mentioned that their top managements are SOMETIMES reviewing and approving the ISM plans.

**Third Question: How important is the support received from Top Management for the success of managing the Information Security?** This question is the main question of this section. The comparative analysis between Jordanian and Finnish organizations will be tested by this question. This question investigates the importance of the top management support as a critical factor for the success of ISM. The following figure displays distribution of the importance of this factor. The x axis represents the importance of top management support as success factor, while the y axis represents the percentage of respondents.



**Figure 5- 5** *Importance of the top management support*

As presented by the above figure, 53.45% (31 respondents) respondents have ranked the top management support as important factor for the success of ISM, 39.66% (23 respondents) as an extremely important factor, 1.72% (one response) as weakly important factor, and 1.72% (one respondent) as not important factor. Finally this question was not applicable for 3.45% (two respondents). As shown above, high percentage of respondents considers top management support as an integral component of ISM's success. This confidence may come from their belief that top management can offer an adequate support for ISM plans.

**Testing Hypothesis**

*H1.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of top management support for the success of ISM.*

The hypothesis of this factor is **supported**. The Asymptotic Significance of continuity correction value is .037. This indicates that the relation *is significantly different* and the Hypothesis of this factor is **supported**. In other words, the proportion of the Jordanian respondents is *significantly different* from the proportion of the Finnish respondents toward the importance of this factor.

**Table 5- 4** *Chi-Square test of Top management support factor*

<b>Chi-Square Tests</b>					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5.540 <sup>b</sup>	1	.019		
Continuity Correction <sup>a</sup>	4.332	1	.037		
Likelihood Ratio	5.616	1	.018		
Fisher's Exact Test				.029	.018
Linear-by-Linear Association	5.441	1	.020		
N of Valid Cases	56				

a. Computed only for a 2x2 table

b. 0 cells (.0%) have expected count less than 5. The minimum expected count is 10.68.

As can be seen from the next table, there are 50% (35.7% + 14.3%) of the Finnish respondents that have classified this factor as important and extremely important. While 46.4% (19.6% + 26.8%) of the Jordanian respondents have classified this factor as important and extremely important. Since the hypothesis of this factor is **supported**, the significant difference shows that this factor is more important for the Finnish companies than Jordanian companies. This result would be convinced because the top managements of Finnish companies, as developed country, are realizing the importance of information security and this could be one of the reasons that converted the Finnish market to be one of the leaders in the IT sector worldwide. However, top managements of Jordanian companies have also shown a high importance regard ISM.

**Table 5- 5** Cross tabulation of Top Management support factor for Jordan and Finland

**Group (Finland - Jordan) \* (Top Management Support) Crosstabulation**

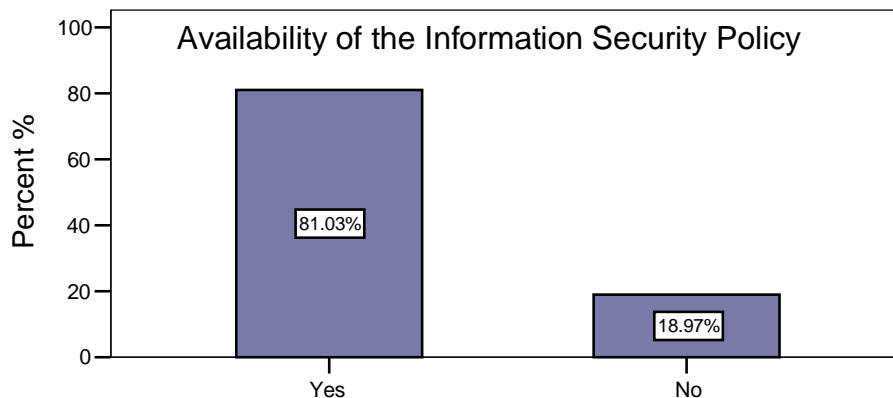
			Top Management Support (TMS)				Total
			Not Important	Weakly Important	Important	Extremely Important	
Group	Finland	Count	1	1	20	8	30
		Expected Count	,5 <sup>a</sup>	,5	16,6	12,3	30,0
		% within Group	3,3%	3,3%	66,7%	26,7%	100,0%
		% within (TMS)	100,0%	100,0%	64,5%	34,8%	53,6%
		% of Total	1,8%	1,8%	35,7%	14,3%	53,6%
	Jordan	Count	0	0	11	15	26
		Expected Count	,5	,5	14,4	10,7	26,0
		% within Group	,0%	,0%	42,3%	57,7%	100,0%
		% within (TMS)	,0%	,0%	35,5%	65,2%	46,4%
		% of Total	,0%	,0%	19,6%	26,8%	46,4%
Total	Count	1	1	31	23	56	
	Expected Count	1,0	1,0	31,0	23,0	56,0	
	% within Group	1,8%	1,8%	55,4%	41,1%	100,0%	
	% within (TMS)	100,0%	100,0%	100,0%	100,0%	100,0%	
	% of Total	1,8%	1,8%	55,4%	41,1%	100,0%	

a. Red highlighted cells that have expected count less than 5, are combined with relative cell other columns in order to run the Chi-Square test.

#### 5.4.2 Information Security Policy (ISP)

This section shows the perspectives of respondents towards the importance of ISP factor for success of ISM. This section spells three questions. First question explores availability of ISP. Second question investigates the importance of ISP for the success of ISM. This question will be used for comparative analysis between Jordanian and Finnish companies. Third question inquires the importance of support received from the end-users for the successful implementation of ISP.

**First Question: Does your organization have a formal Information Security Policy?** ISP is a demonstrative tool to express and communicate the ISM activities. The figure below shows the availability of ISP within the organizations. The x axis represents the ISP availability which is scaled by Yes and No. The y axis shows the percentage of the respondents.

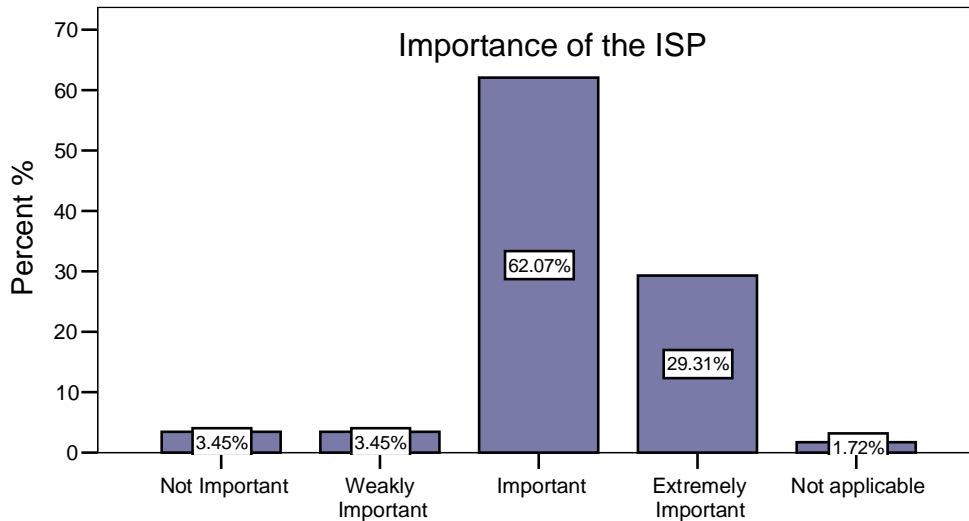


**Figure 5- 6** *Availability of the ISP*

Based on the above figure, there are 81.03% (47 respondents) respondents that have adopted an ISP in their companies, while 18.97% (11 respondents) respondents have not adopted an ISP. It seems that a high portion of respondents companies are realizing the return benefits of adopting ISP.

Within the companies that have an ISP, 54.4% consider ISP as an important while 24.6% consider ISP as extremely important factor for ISM success. Within the companies that do not have an ISP, 17.5% consider ISP as an important factor for ISM success (see table 5-23, appendix C).

**Second Question: How important is the information security policy for managing information security in your organization?** This question is the main question of this section. The comparative analysis between Jordanian and Finnish organization will be tested by this question. This question explores the perspective of the respondents towards the importance of ISP for managing information security. The figure below shows the importance of ISP as success factor which represented by x axis. The y axis shows the percentage of the respondents.



**Figure 5- 7** *Importance the ISP*

As presented by the above figure, 62.07% (36 respondents) respondents have ranked the ISP as important factor for the success of ISM, 29.31% (17 respondents) as an extremely important factor, 3.45% (2 respondents) as weakly important factor, and 3.45% (2 respondent) as not important factor. Finally this question was not applicable for 1.72% (one respondent).

### **Testing Hypothesis**

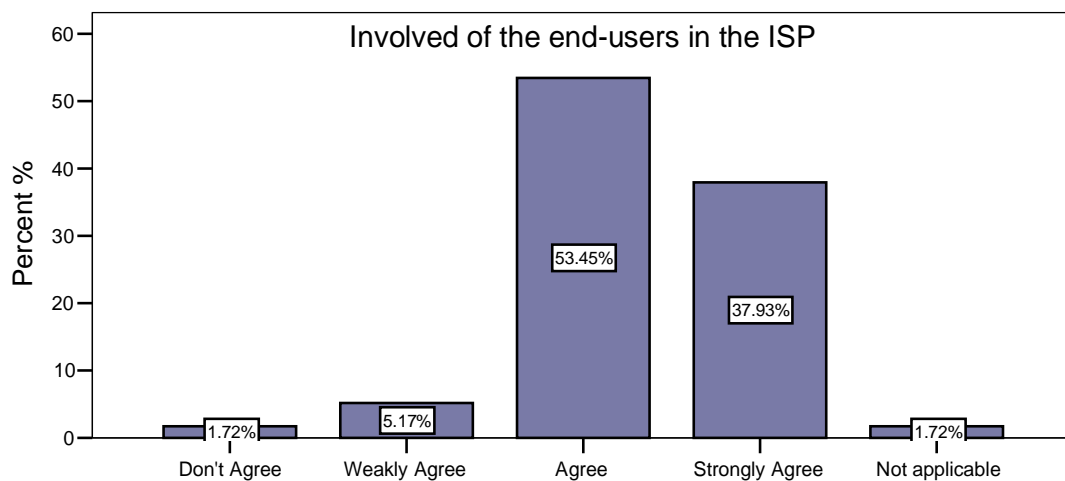
**H2.1:** *There is a significant difference between Jordanian and Finnish observations regarding the importance of ISP for the success of ISM.*

The hypothesis of this factor is **supported**. The Asymptotic Significance of continuity correction value is .046. This indicates that the relation **is significantly different** and the Hypothesis of this factor is **supported**. In other words, the proportion of the Jordanian respondents is **significantly different** from the proportion of the Finnish respondents toward the importance of this factor (see table 5-6, appendix B).

As presented in table 5-7 in appendix B, there are 47.4% (38.6% + 8.8%) of the Finnish respondents that have classified this factor as important and extremely important. While 45.7% (24.6% + 21.1%) of the Jordanian respondents have classified this factor as important and extremely important. Since the hypothesis of this factor is **supported**, the significant difference shows that this factor is more important for the Finnish companies than Jordanian companies. As can be noticed, the

Finnish companies are significantly classifying this factor to be important more than Jordanian companies. Even there is a significant difference between Jordanian and Finnish companies but both of them are quite aware about the importance of ISP for success of ISM.

**Third Question: Do you agree that sufficient support from the end-users is critical to the successful implementation of the Information Security policy?** This question explores role of end-users towards support ISP implementation. The figure below shows the points of views of the respondents towards involvement of the end-users to success of ISP implementation. The x axis represents the perspectives of the respondents. While the y axis represents the percentage of respondents.



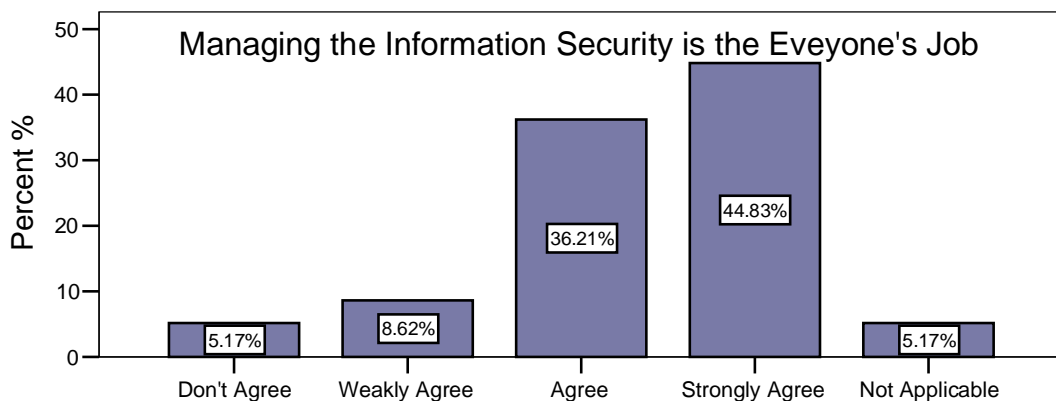
**Figure 5- 8** Support and involved of the end-users in the ISP

As presented by the above figure, 53.45% (31 respondents) respondents that have agreed the involvement and support of end-users are important to success of ISP implementation, 37.93% (22 respondents) as strongly agreed, 5.17% (3 respondents) as weakly agreed, 1.72% (one response) as not agreed. Finally, this question was not applicable for 1.72% (one respondent). These results show that ISP implementation is highly influenced by support and involvement of end-users.

### 5.4.3 Job Responsibilities

This section shows the perspectives of respondents towards the importance of Job Responsibilities as a success factor managing information security. This section spells two questions. First question explores whether managing information security is everyone's job. Second question investigates the importance of Job Responsibilities for the success of ISM. This question will be used for comparative analysis between Jordanian and Finnish companies.

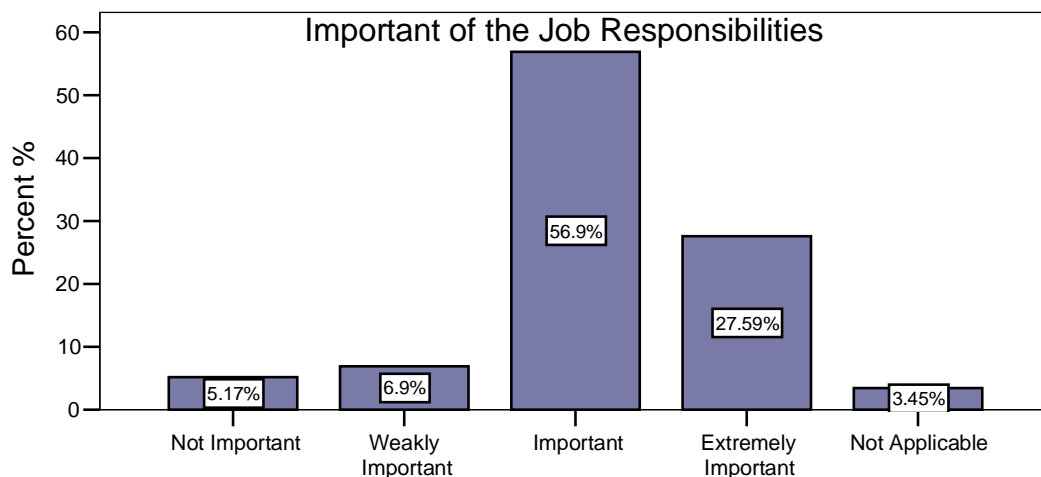
**First Question: Do you agree that managing information security is everyone's job?** This question explores whether ISM is everyone's job. The next figure shows the opinion of respondents towards ISM responsibility. The x axis represents the frequency of agreement. The y axis represents the percentage of respondents.



**Figure 5- 9** *Information security is everyone's job*

As can be seen from the above figure, 36.21% (21 respondents) respondents have agreed that managing information security is everyone's job, 44.83% (26 respondents) as strongly agreed, 8.62% (5 respondents) as weakly agreed, 5.17 % (3 respondents) as not agreed. Finally, this question was not applicable for 5.17 % (3 respondents). There are high percentages of respondents are agreed and strongly agreed that managing information security is everyone's job.

**Second Question: Is defining the information security responsibilities in advance for each job important for success of managing the Information security?** This question is the main question of this section. The comparative analysis between Jordanian and Finnish organizations will be tested by this question. This question explores the perspective of the respondents towards the importance of Job Responsibilities for managing information security. The figure below shows the importance of Job Responsibilities as success factor for managing information security. The x axis represents the importance of Job Responsibilities. The y axis shows the percentage of the respondents.



**Figure 5- 10** *Importance of the job responsibilities*

As presented by the above figure, 27.59% (16 respondents) respondents have ranked the Job Responsibilities as extremely important factor for the success of ISM, 65.9% (33 respondents) as an important factor, 6.9% (4 respondents) as weakly important factor, and 5.17% (3 respondent) as not important factor. Finally this question was not applicable for 1.72% (one respondent).

**Testing Hypothesis**

*H3.1: There is a significant difference between Jordanian and Finnish respondents regarding the importance of job responsibilities for the success of ISM.*

The hypothesis of this factor is *partly supported*. The Asymptotic Significance of continuity correction value is .068. This indicates that the relation is *weakly significantly different* and the Hypothesis of this factor is *partly supported*. In other words, the proportion of the Jordanian respondents is *weakly significantly different* from the proportion of the Finnish respondents toward the importance of this factor (see table 5-8 appendix B).

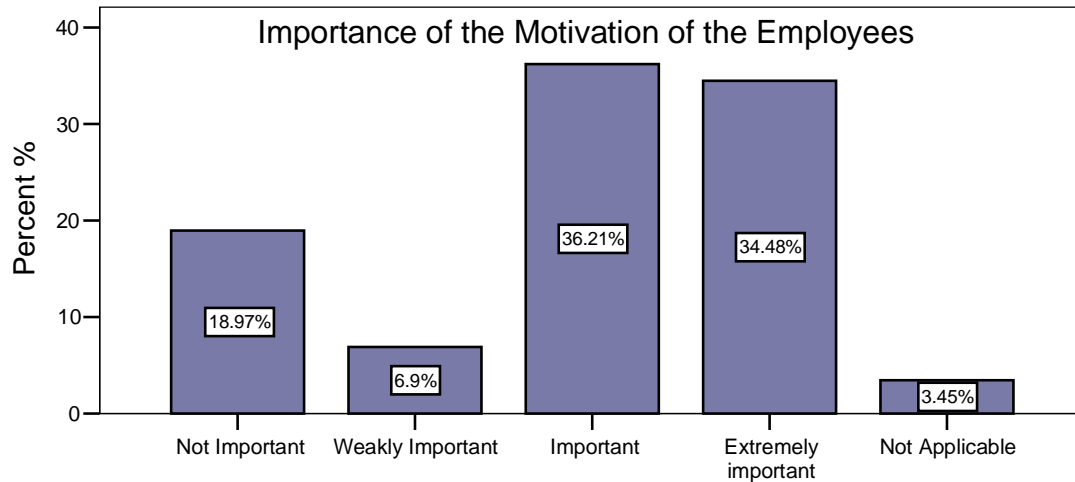
As presented in table 5-9 appendix B, there are 53.6% (35.7% + 8.9%) of the Finnish respondents that have classified this factor as important and extremely important. While 46.7% (23.2% + 19.6%) of the Jordanian respondents have classified this factor as important and extremely important. Since the hypothesis of this factor is **partly supported**, it has been classified to be relatively important for Finnish and Jordanian companies. It seems Finland and Jordan companies are conscious towards importance of allocating information security responsibility to be one of main priorities of everyone's job.

#### 5.4.4 Motivation of Employees

This section shows the perspectives of respondents towards the importance of motivation of employees for success of ISM. This section spells three questions. First question explores importance of motivation of employees as success factor for ISM. Second question investigates whether rewarding and appreciation systems will increase security conscious amongst of employees. Third question inquires if the respondents companies have rewarding or appreciation systems.

**First Question: How important is the motivation of the employees for the success of managing information security?** This question is the main question of this section. The comparative analysis between Jordanian and Finnish organizations will be tested by this question. This question explores the perspective of the respondents towards the importance of motivation of employees for managing information security. The figure below shows the importance of motivation of employees as

success factor for ISM. The x axis represents the importance of motivation of employees. The y axis shows the percentage of the respondents.



**Figure 5- 11** *Importance of the motivation of the employees*

As presented by the above figure, 34.48% (20 respondents) respondents have ranked motivation of employees as extremely important factor for the success of ISM, 36.21 % (21 respondents) as an important factor, 6.9% (4 respondents) as weakly important factor, and 18.97% (11 respondents) as not important factor. Finally this question was not applicable for 3.45% (2 respondents).

### **Hypothesis Testing**

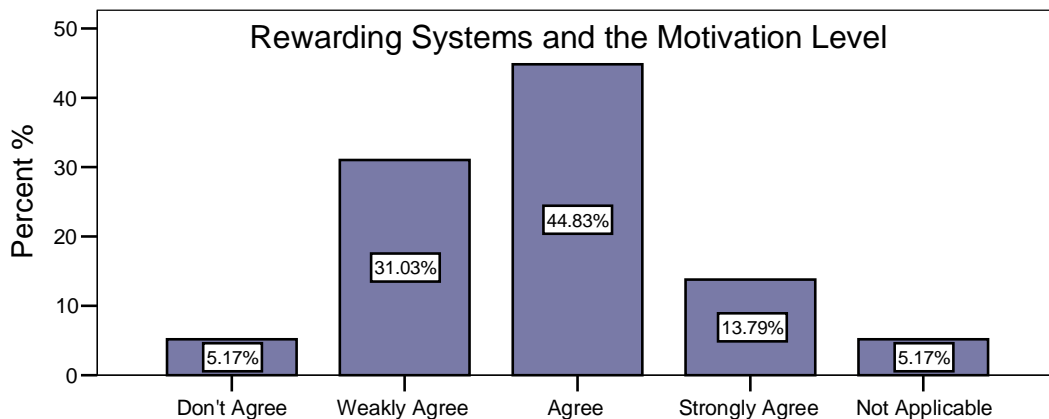
*H4.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of motivation of employees for the success of ISM.*

The hypothesis of this factor is **rejected**. The Asymptotic Significance of Pearson chi-square value is .277. This indicates that the relation **is no significantly different** and the Hypothesis of this factor is **rejected**. In other words, the proportion of the Jordanian respondents is **not significantly different** from the proportion of the Finnish respondents toward the importance of this factor (see table 5-10, appendix B).

As presented in table 5-11 in appendix B, there are 35.8% (17.9% + 17.9%) of the Finnish respondents that have classified this factor as important and extremely

important. While 37.5% (19.6% + 17.9%) of the Jordanian respondents have classified this factor as important and extremely important. Since the hypothesis of this factor is **rejected**, this factor has been classified to be of same important for Finnish companies as to Jordanian companies. It seems the respondents companies, in Finland or Jordan, are realizing that motivation of employees increase consciousness towards ISM issues.

**Second Question: Do you agree that such a reward or appreciation system would increase the motivational level among the employees and they would become more security conscious?** This question investigates the respondents' perspectives towards adopt reward and appreciation systems as motivational method. The figure below illustrates the views of respondents regarding the importance of reward and appreciation systems. The x axis represents the perspectives of the respondents, while the y axis represents the percentage of respondents.



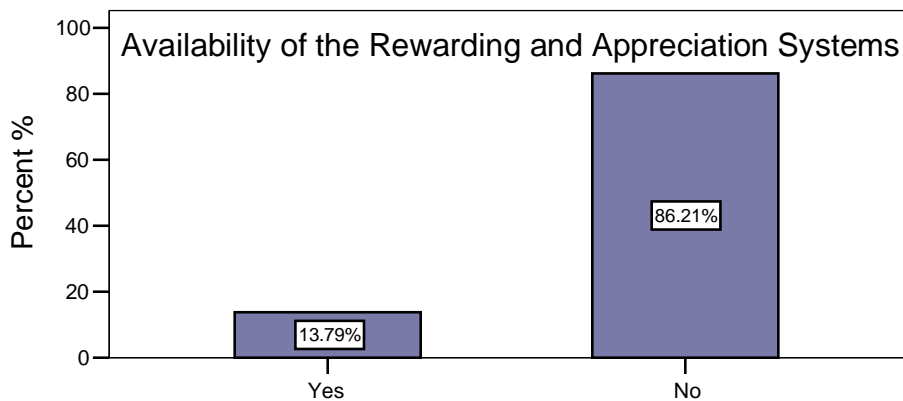
**Figure 5- 12** *Reward and Appreciation Systems and the Motivation Level*

As can be seen from the above figure, 44.83% (26 respondents) respondents have agreed that rewarding and appreciation will increase the information security conscious amongst the employees. 13.79% (8 respondents) as strongly agreed, 31.03% (18 respondents) as weakly agreed, 5.17 % (3 respondents) as not agreed. Finally, this question was not applicable for 5.17 % (3 respondents). There is a high

percentage of the respondents agree and strongly agree that rewarding and appreciation systems will increase the motivation level amongst employees.

**Question Three: Is there any reward or appreciation system in your organization for those who perform well on Information Security Management (ISM)?**

Availability of rewarding and appreciation systems is important to make employees pay attention for information security. The figure below shows the availability of rewarding and appreciations systems within the organizations. The x axis represents the availability these systems which is scaled by Yes and No. The y axis shows the percentage of the respondents.



**Figure 5- 13** *Availability of the reward and appreciation systems*

As can be noticed from the above figure, there are 86.21% (50 respondents) respondents do not have rewarding and appreciation systems in their companies, while 13.79% (8 respondents) respondents have adopted rewarding and appreciation systems. It seems that a little portion of respondents companies are realizing the return benefits of adopting these systems.

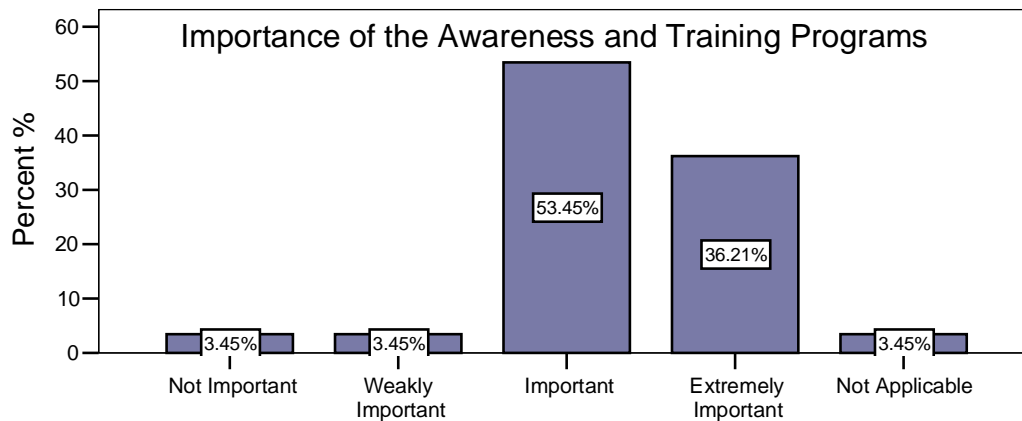
First and second questions of this section show positive perspective regarding importance of these systems (rewarding and appreciations systems). According to figure 5-11, 36.21% and 34.48% of the respondents indicated that motivation of

employees is important and extremely important for the success of ISM. According to figure 5-12, 44.84% and 13.79% of the respondents agreed and strongly agreed that rewarding and appreciation systems positively influence the employees to be conscious towards information security. Although, a high percentages of respondent advocated motivation of employees as an important factor, there are 86.21% of respondents companies that do not have any rewarding systems (figure 5-13).

#### 5.4.5 Awareness and Training programs

This section shows the perspectives of respondents towards the importance of awareness and training programs for success of ISM. This section spells three questions. First question explores importance of awareness and training programs as success factor for ISM. Second question investigates whether respondents companies are implementing awareness and training programs. Third question explores if respondents companies, who have implemented awareness and training programs, are relying on external parties to manage these programs.

**First Question: How important are Awareness and Training Programs for the successful management Information Security?** This question is the main question of this section. The comparative analysis between Jordanian and Finnish organizations will be tested by this question. This question explores the perspective of the respondents towards the importance of awareness and training programs for managing information security. The figure below shows the importance of these programs which scaled by the x axis. The y axis shows the percentage of the respondents.



**Figure 5- 14** *importance of the awareness and training programs*

As presented by the above figure, 53.45% (31 respondents) respondents have ranked awareness and training programs as important factor for success of ISM, 36.21 % (21 respondents) as an extremely important factor, 3.45% (2 respondents) as weakly important factor, and 3.45% (2 respondents) as not important factor. Finally this question was not applicable for 3.45% (2 respondents).

### **Testing Hypothesis**

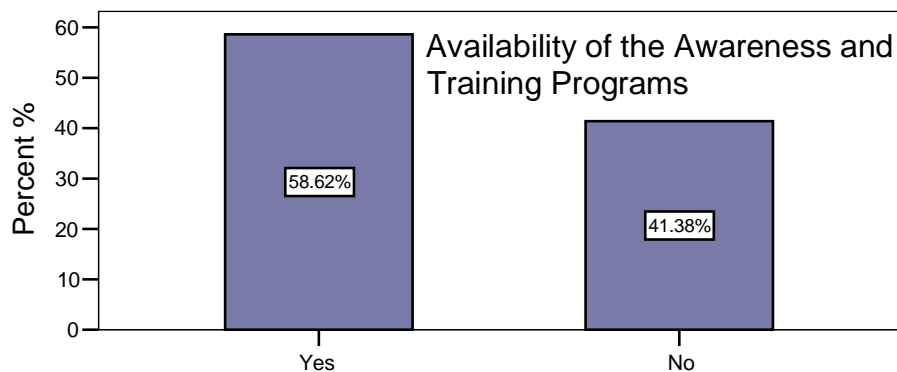
*H5.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of awareness and training programs for the success of ISM.*

The hypothesis of this factor is **rejected**. The Asymptotic Significance of continuity correction value is .581. This indicates that the relation **is not significantly different** and the Hypothesis of this factor is **rejected**. In other words, the proportion of the Jordanian respondents is **not significantly different** from the proportion of the Finnish respondents toward the importance of this factor (see table 5-12, appendix B).

As presented in table 5-13 in appendix B, there are 28.6% and 16.1% of the Finnish respondents that have classified this factor as important and extremely important. While 28.6% and 21.4% of the Jordanian respondents have classified this factor as important and extremely important. Since the hypothesis of this factor is **rejected**, this

factor has been classified to be of same important for Finnish companies as to Jordanian companies. It seems the respondents companies, in Finland or Jordan, are appreciating the importance of awareness and training programs for success of ISM.

**Second Question: Has your organization implemented any Information security awareness and training program?** Availability of awareness and training programs is important for the success of ISM. The figure below shows the availability of these programs within the organizations. The x axis represents the availability of these programs which is scaled by Yes and No. The y axis shows the percentage of the respondents.

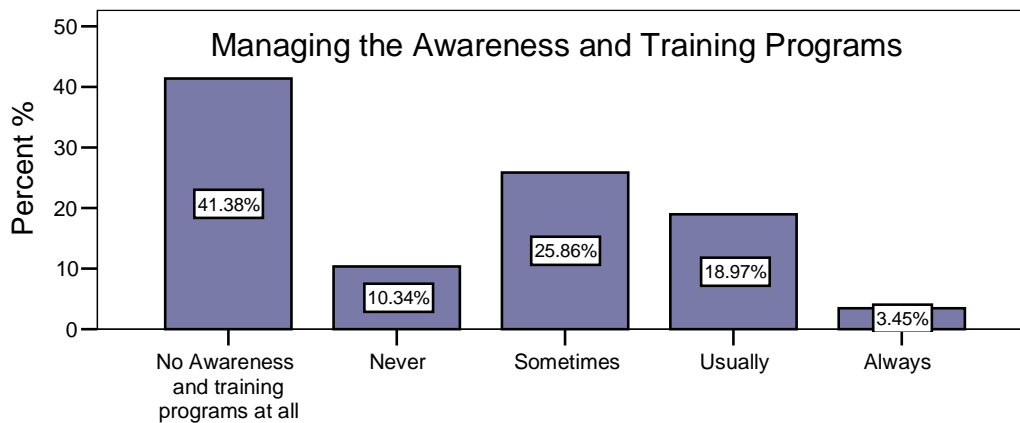


**Figure 5- 15** Availability of the awareness and training programs

As can be noticed from the above figure, there are 58.62% (34 respondents) respondents have awareness and training programs in their companies, while 41.38% (24 respondents) respondents do not have adopted awareness and training programs. It seems that a more than half of respondents companies are using to adopt these programs.

Within the companies that do not have an awareness and training programs, 28.6% consider these programs as an important and 7.1% consider them as extremely important factor for ISM success (see table 5-24, appendix C). This means these programs are absolutely important for managing information security in the organizations, but it seems many of these organizations are escaping these programs.

**Third Question: Does your organization manage the Awareness and Training programs without the help of outside organizations?** Managing awareness and training programs is very important which reflects the perspective of organizations towards custody of information security awareness. As presented in figure 5-15, 58.62% (34 responses) respondents have awareness and training programs in their companies. These respondents have answered this question. The next figure shows the frequency of managing these programs without help of outside of organization. The x axis represents the frequency of managing these programs. The y axis represents the percentage of respondents.



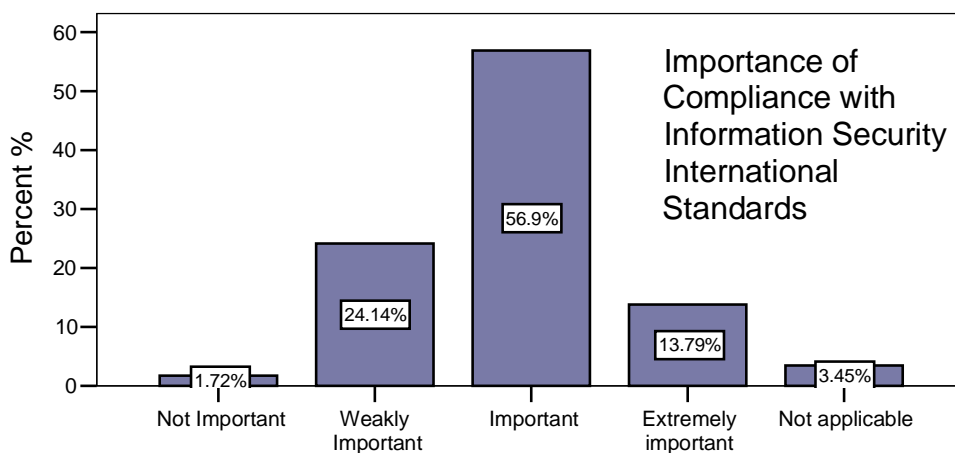
**Figure 5- 16** *Managing the awareness and training programs*

As displayed by the above figure, 41.38% (24 respondents) do not have awareness and training programs in their companies. 10.34% (6 respondents) are NEVER relying on outside organizations to manage their awareness and training programs. 25.86% (15 respondents) are SOMETIMES relying on outside parties to hold such these programs. 18.97% (11 respondents) are USUALLY and 3.45% (2 respondents) are ALWAYS relying on outside organizations to hold their awareness and training programs.

#### 5.4.6 Compliance with information security international standards

This section shows the perspectives of respondents towards the importance of information security international standards for success of ISM. This section spells three questions. First question explores importance of information security international standards as success factor for ISM. Second question investigates whether respondents companies are implementing these standards. Third question asks whether competitive advantage is gained by adopting these standards

**First Question: How important is the compliance with International Standards of Information Security for the overall success of Information Security Management within your organization?** This question is the main question of this section. The comparative analysis between Jordanian and Finnish organizations will be tested by this question. This question explores the perspective of the respondents towards the importance of compliance with information security international standards for managing information security. The figure below shows the importance of compliance with these standards as success factor for ISM. The x axis represents the importance of these standards. The y axis shows the percentage of the respondents.



**Figure 5- 17** *Importance of compliance with information security international standards*

As presented by the above figure, 56.9% (33 respondents) respondents have ranked compliance with information security international standards as important factor for success of ISM, 13.79 % (8 respondents) as an extremely important factor, 24.14%

(14 respondents) as weakly important factor, and 1.72% (one respondent) as not important factor. Finally this question was not applicable for 3.45% (2 respondents).

### **Testing Hypothesis**

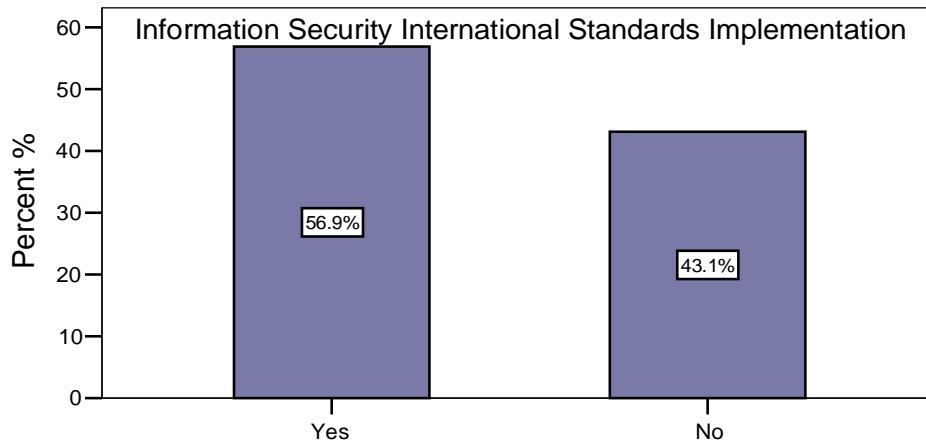
*H6.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of compliance with information security international standards for the success of ISM.*

The hypothesis of this factor is **supported**. The Asymptotic Significance of Pearson Chi-square value is .007. This indicates that the relation *is significantly different* and the Hypothesis of this factor is **supported**. In other words, the proportion of the Jordanian respondents is *significantly different* from the proportion of the Finnish respondents toward the importance of this factor (see table 5-14, appendix B).

As presented in table 5-15 in appendix B, there are 23.2% and 19.6% of the Finnish respondents that have classified this factor as weakly important and important. While 37.5% and 8.9% of the Jordanian respondents have classified this factor as important and extremely important. Since the hypothesis of this factor is **supported**, this factor has been classified to be more important for Jordanian companies than Finnish companies. It seems that the Jordanian companies are realizing the importance of adopting these standards, but that does not mean that the Finnish companies are not considering these standards to manage information security.

### **Second Question: Do you make use of international information security standards for the management of information security in your organization?**

Using the information security international standards is important for the success of ISM. The figure below shows using of these standards within the organizations. The x axis represents using of these standards and is scaled by Yes and No. The y axis shows the percentage of the respondents.



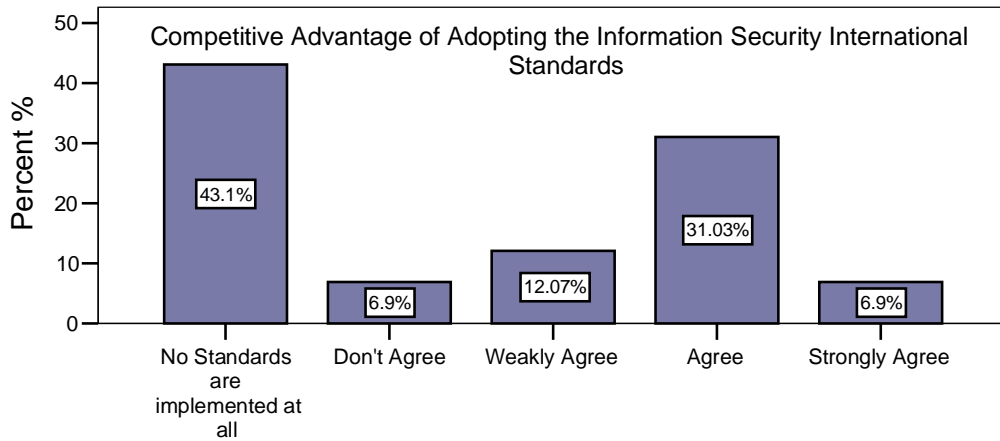
**Figure 5- 18** *The information security international standards implementation*

As can be noticed from the above figure, there are 56.9% (33 respondents) respondents have using information security international standards in their companies, while 43.1% (25 respondents) respondents do not have adopted these standards. It seems that more than half of respondents companies are using to adopt these programs.

Within the companies that do not adopt information security international standards, 14.3%, 23.2% and 3.6% of the respondents have respectively considered adopting these standards as weakly important, important and extremely important for ISM success (see table 5-24, appendix C). Although less than half of respondents companies do not adopt these standards, these standards are absolutely essential for ISM success.

**Third Question: Do you agree that by adopting Information Security International Standards your company gains a competitive advantage?**

Importance of this factor enforces the confidence amongst organizations. The next figure shows whether adopting these standards will make companies gain competitive advantage. The x axis represents agreement of respondents towards these standards to have competitive advantage. The y axis represents the percentage of respondents.



**Figure 5- 19** *Competitive advantage and adopting the information security international standards*

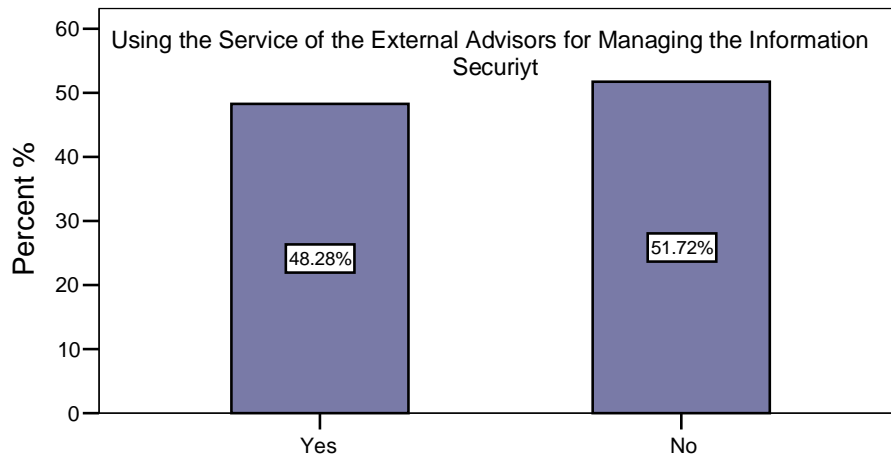
As displayed by the above figure, 43.1% (25 respondents) do not have adopted these standards in their companies. 31.03% (18 respondents) respondents have agreed that compliance with information security international standards will enhance the competitive advantage of organizations. 6.9% (4 respondents) as strongly agreed, 12.07% (7 respondents) as weakly agreed and 6.9% (4 respondents) as not agreed. The majority of respondents have agreed that adopting these standards will give organization competitive advantage.

#### 5.4.7 Using services of information security external advisors

This section shows the perspectives of respondents towards the importance of using services of information security external advisors for success of ISM. This section spells three questions. First question investigates whether the respondents companies are using services of information security external advisors. The second question explores the importance of using these services as success factor for ISM. Third question searches frequency of relying on recruitment agencies to hire and contract with information security specialists.

**First Question: Does your organization use the services of any external parties for managing information security?** The shortage of information security experience and practices inside organizations has induced most of organizations to rely on external parties to manage their information security. This question

investigates whether the respondent companies are using services of information security specialists. The figure below shows using services of information security external parties within the organizations. The x axis represents using these services which is scaled by Yes and No. The y axis shows the percentage of the respondents.



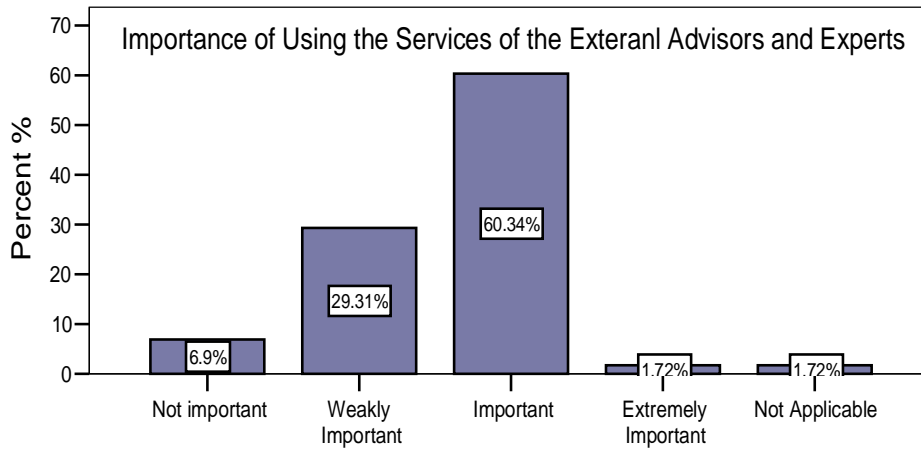
**Figure 5- 20** *Using the service of the external parties for managing information security*

As can be noticed from the above figure, there are 48.28% (28 respondents) respondents that have been using services of information security external advisors in their companies, while 51.72% (30 respondents) respondents do not use services of information security external advisors.

Within the companies that do not have using services of information security external advisors, 31.6% (18 respondents) have considered using services of information security external advisors as important for ISM success (see table 5-26 appendix C).

**Second Question: Do you believe the use of consultants and external advisors plays a part in the success of managing your organizations' information security?** This question is the main question of this section. The comparative analysis between Jordanian and Finnish organizations will be tested by this question. This question explores the perspective of the respondents towards the importance of using services of information security external advisors. The figure below shows the importance of using these services as success factor for ISM. The x axis represents the

importance of using these services. The y axis shows the percentage of the respondents.



**Figure 5- 21** Importance of using services of information security external advisors

As presented by the above figure, 60.34% (35 respondents) respondents have classified using services of information security external advisors as important factor for success of ISM, 29.31 % (17 respondents) as an weakly important factor, 6.9% (4 respondents) as not important factor, and 1.72% (one respondent) as extremely important factor. Finally this question was not applicable for 1.72% (one respondent).

### **Testing Hypothesis**

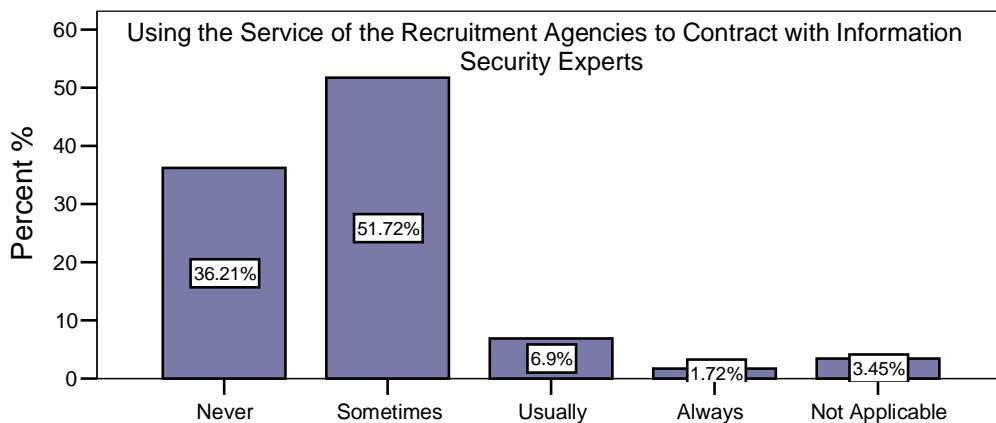
*H7.1: There is a significant difference between Jordanian and Finnish observations regarding the importance of using services of information security external advisors for the success of ISM.*

The hypothesis of this factor is **rejected**. The Asymptotic Significance of continuity correction value is .178. This indicates that the relation **is not significantly different** and the Hypothesis of this factor is **rejected**. In other words, the proportion of the Jordanian respondents is **not significantly different** from the proportion of the Finnish respondents toward the importance of this factor (see table 5-16, appendix B).

As presented in table 5-17 in appendix B, there are 19.3% and 26.3% of the Finnish respondents that have classified this factor as important and extremely important. While 10.5% and 35.1% of the Jordanian respondents have classified this factor as

important and extremely important. Since the hypothesis of this factor is **rejected**, this factor has been classified to be of same important for Finnish companies as to Jordanian companies. Using service of external information security advisors would be very helpful for companies. Companies will be able to manage their information security perfectly, and enhance knowledge of their internal staff which minimizes need for external support in future.

**Third Question: Does your company use the services of recruitment agencies in order to hire and contract with information security experts?** Recruiting information security employees is hard mission. Therefore, some organizations contract with recruitment agencies to assist them in hiring qualified employees that can fulfil organizations' information security requirements. The next figure displays the frequency of relying on recruitment agencies to hire employee that can fulfil organizations' information security requirements. The x axis represents the frequency of relying on recruitment agencies. The y axis represents the percentage of the respondents.



**Figure 5- 22** *Using the services of the recruitment agencies.*

As displayed by the above figure, 36.21% (21 respondents) are NEVER relying on recruitment agencies. 51.72% (30 respondents) are SOMETIMES relying recruitment agencies. 6.9% (4 respondents) are USUALLY and 1.72% (one respondent) is ALWAYS relaying on recruitment agencies. This question was not applicable for 3.45% (2 responses).

## 5.5 Testing the second part of hypotheses (importance of the success factors of ISM)

As mentioned earlier, this study has two parts of hypotheses. The first part has already been tested. This section shows the results of testing the second part of the hypotheses.

The second part of the previously developed hypotheses assumes that all the mentioned factors are important for managing the information security. Table 5-1 displays the survey questions used to test these hypotheses. T-test (one-sample statistics) is used to test the validity of these hypotheses.

The importance of these factors were investigated based on the following scale of importance: (1) Not Important, (2) Weakly Important, (3) Important and (4) Extremely Important. If the Average of these factors is more than 3, then the factor will be classified as important and its hypothesis will be considered as *supported*. If the mean is between 2 and 3, the factor will be ranked as weakly important and its hypothesis will be considered as *partly supported*. The hypothesis will be rejected if the mean is less than 2.

Table 5-18 shows that the support received from the top management is the most important factor amongst all the other success factors. The Average of 3.41 is the largest among all averages. On the other hand, using services of information security external advisors is classified as the least importance factor, as its mean is the lowest (2.63) among other success factors.

**Table 5- 18** *Statistical results of testing second part of hypotheses*

<b>Factor/ Hypothesis</b>	<b>Mean</b>	<b>Std. Deviation</b>	<b>Result</b>
Top Management Support <b>(H 1.2)</b>	3.41	.496	<b>Supported</b>
Awareness and Training Programs <b>(H 5.2)</b>	3.38	.489	<b>Supported</b>
Information Security Policy <b>(H 2.2)</b>	3.30	.462	<b>Supported</b>
Job Responsibilities <b>(H 3.2)</b>	3.16	.626	<b>Supported</b>
The Motivation of the Employees <b>(H 4.2)</b>	2.89	1.107	<b>Partly Supported</b>
Compliance with Information Security International Standards and guidelines <b>(H 6.2)</b>	2.88	.689	<b>Partly Supported</b>
Using Services of Information Security External Advisors <b>(H 7.2)</b>	2.63	.487	<b>Partly Supported</b>

## **6. CONCLUSION**

### **6.1 Validity, Reliability and Generalizability**

Online survey was the main instrument used to collect data. I used an online survey provider service, Webropol Oy, to collect data. The survey was sent to Chief Information Officers (CIO) and Internal Auditing Department heads. It was sent to 85 Jordanian companies and 152 Finnish companies. Out of these, 28 companies from Jordan and 30 from Finland responded. The response rate was, thus, 33% for Jordanian companies and 20% for Finnish companies. Initial analysis of respondents showed that respondents had an average experience of three to fifteen years in information security assignments.

The research survey was circulated among PhD students for expert comments before sending it out to respondents. The comments received from PhD students were incorporated in survey before finalizing it for final draft.

I deliberately chose Jordan and Finland for this study, as both are at a different level of economic development. Therefore, I expect Jordanian and Finnish companies to be at a different level of organizational development as well. This difference resulted in causing the difference about importance of factors under discussion between Jordanian and Finnish companies. I expect these differences to go away as Jordanian companies become more developed and mature.

### **6.2 Discussion and Summery**

Fourteen hypotheses have been developed in this study. Seven of them were used to document the importance of these factors for ISM success and remaining seven tested whether these factors hold different relative importance in Jordan and Finland

Online survey was used to gather data from both countries. Response rate was 20% in Finland and 33% in Jordan (see table 4-2). SPSS was used to test hypotheses using parametric and non-parametric tests.

The results show that most of the respondent companies are employing a large number of employees. It was also documented that only 7 companies among my sample have a separate ISM department. 49 companies were tackling ISM under IT department, while 2 companies designated this responsibility to HR and Finance departments. Majority of the targeted respondent titles have years of experience between 3 and 15 years with information security assignments.

**Table 6- 1** *Summery of tested hypotheses*

<b>Factor</b>	<b>Hypotheses</b>	<b>Mean (independent-test)</b>	<b>Sig. (chi-test)</b>	<b>Result</b>	<b>Rank</b>
Top Management Support	H 1.1	-----	.037	<b>Supported</b>	<b>1</b>
	H 1.2	3.41	-----	<b>Supported</b>	
Information Security Policy	H 2.1	-----	.046	<b>Supported</b>	<b>3</b>
	H 2.2	3.30	-----	<b>Supported</b>	
Job Responsibilities	H 3.1	-----	.068	<b>Partly Supported</b>	<b>4</b>
	H 3.2	3.16	-----	<b>Supported</b>	
The Motivation of the Employees	H 4.1	-----	.277	<b>Rejected</b>	<b>5</b>
	H 4.2	2.89	-----	<b>Partly Supported</b>	
Awareness & Training Programs	H 5.1	-----	.581	<b>Rejected</b>	<b>2</b>
	H 5.2	3.38	-----	<b>Supported</b>	
Compliance with Information Security International Standards and guidelines	H 6.1	-----	.007	<b>Supported</b>	<b>6</b>
	H 6.2	2.88	-----	<b>Partly Supported</b>	
Using Services of Information Security External Advisors	H 7.1	-----	.178	<b>Rejected</b>	<b>7</b>
	H 7.2	2.63	-----	<b>Partly Supported</b>	

Two types of hypotheses were investigated. First type examined comparative analysis between Jordanian and Finnish companies and second explored the importance of success factors for ISM. The results have shown that three factors (i.e. Top management support, ISP, and Compliance with information security international standards) are significantly of different importance for Jordanian and Finnish companies.

- A. **Top management support:** my results show that there is statistically significant difference between Jordanian and Finnish companies regarding the importance of top management support in ISM success. Moreover, my results document that Finnish companies rank top management support as a more important factor in ISM success than their Jordanian counterparts (table 5-5). Furthermore, I show that this factor is the most important factor in ISM success in comparison with all of other discussed factors.
- B. **Information Security Policy:** my results show that there is statistically significant difference between Jordanian and Finnish companies regarding the importance of ISP in ISM success. Moreover, my results document that Finnish companies rank information security policy as a more important factor in ISM success than their Jordanian counterparts (see table 5-7). Furthermore, I show that this factor is the third important factor in ISM success in comparison with all of other discussed factors.
- C. **Job Responsibilities:** my results show that there is statistically weakly significant difference between Jordanian and Finnish companies regarding the importance of Job Responsibilities for success of ISM. Moreover, my results document that this factor has been classified to be of relatively important for Finnish companies as to Jordanian companies (see table 5-9). Furthermore, I show that this factor is the fourth important factor in ISM success in comparison with all of other discussed factors.
- D. **Motivation of employees:** my results show that there is statistically no significant difference between Jordanian and Finnish companies regarding the importance of motivation of employees for success of ISM. Moreover, my results document that this factor has been classified to be of same important for Finnish companies as to Jordanian companies (see table 5-11). Furthermore, I show that this factor is the fifth important factor in ISM success in comparison with all of other discussed factors.

- E. **Awareness and training programs:** my results show that there is statistically no significant difference between Jordanian and Finnish companies regarding the importance of awareness and training programs for success of ISM. In addition, my results document that this factor has been classified to be of same important for Finnish companies as to Jordanian companies (table 5-13). Furthermore, I show that this factor is the second important factor in ISM success in comparison with all of other discussed factors.
- F. **Compliance with information security international standards:** my results show that there is statistically significant difference between Jordanian and Finnish companies regarding the importance of compliance with information security international standards for success of ISM. Moreover, my results document that Jordanian companies rank this factor as a more important factor in ISM success than there Finnish counterparts (see table 5-15). In addition, I show that this factor is the sixth important factor in ISM success in comparison with all of other discussed factors.
- G. **Using services of information security external advisors:** my results show that there is statistically no significant difference between Jordanian and Finnish companies regarding the importance of using services of information security external advisors for success of ISM. Moreover, this factor has been classified to be of same important for Finnish companies as to Jordanian companies (see table 5-17). In addition, I show that this factor is the seventh important factor in ISM success in comparison with all of other discussed factors.

### 6.3 Analysis of study contribution

Most of the factors discussed in my study have been considered as integral to the success of ISM. For example, Kankanhalli et.al (2003) and Bjorck (2001) discuss the importance of all of these factors in the success of ISM. However, none of the studies, to the best of my knowledge make comparative analysis between developing and developed countries regarding the relative importance of these factors. This study will enhance the point of views of information security specialists towards managing information security in different countries with different levels of educational, economical, technological development. Thus, my study ends a long with the next further research suggestion.

### 6.4 Further research suggestions

This study has shown that the Jordanian and Finnish companies are paying high attention for managing information security. The results show that these countries are significantly different from each other regarding importance of some factors. Having a wider comparison between several countries should be conducted and investigated, since it is important to investigate the reasons stand behind these significant differences.

## 7. References

### E-Articles:

- Bjorck Fredrik, Security Scandinavian Style, Interpreting the Practice of Managing Information Security in Organizations, Stockholm University & Royal Institute of Technology, 2001
- Eloff Jan and Mariki Eloff, Information security management – A new paradigm, ACM, 2003, pages 130-136
- Farahmand Fariborz, Shamkant B Navthe, Gunter P sharp and Philip H Enslow, Managing Vulnerabilities Of information systems to security incidents, ACM, 2003.
- Finne Thomas, A conceptual Framework for information security management, Computer & Security pp 303-307, 1998
- Gonzalez Jose j, Agata Sawicka, A Framework For Human Factors in Information security, WSEAS, Conf on information security, Rio de Janeiro, 2002
- Hone Karin and J.H.P Eloff, Information security policy what do international information security standards say?, Department of Computer Science, Rand Afrikaans University, 2002
- Hinson Gary, Human factor in information security, IsecT Ltd, 2003
- Hong Kwo-shing, Yen-Ping Chi, Louis R. Chao and Jih-Hsing Tang, An integrated System theory of Information Security Management, Information Management & Computer Security, 2003 pp 243-248
- Karyda Maria, Evangelos Kiountouzis and Spyros Kokolakis, Information system security Policies contextual perspective, Computer & Science, 2004 pages 246-260
- Kankanhalli Atreyi, Hock-hai Teo, Bernard C.Y.Tan, and Kwok-kee Wei An integrative study of information systems security effectiveness, international Journal of information management, 2003 pages 139-154
- Koacich Gerald, Establishing an Information systems security organization (ISSO), Computer & Security, 17 (1998) 600-612
- Kwok Lam-for and Dennis Longley, Information Security Management and Modelling information Management & Computer Security, 1999 30-39.
- Lau Oliver, The Ten Commandments of Security, computer & security, 17 (1998) 119-123

Mitchell Ruth C., Rita Marcella and Craeme Baxter, Corporate Information Security Management, New Library World, 1999 pp 213-227

Nosworthy Julie D, Implementing information security in the 21<sup>st</sup> century – Do You Have the Balancing Factors?, computer & security 19 (2000) 337-2347

Siponen Mikko T., Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods, Information and organization, 2005

Solms Rossouw Von, Information security management: the second generation, Computer and Security, 15 (1996) 281-288

Solms Rossouw von, information Security management (1): why information security is so important, information management & computer security, 1998 pp 174-177.

Solms Rossouw von, Information Security Management (2): guidelines to the management of information technology security (GMITS), information management & Computer Security, 1998 pp 221-223.

Solms Rossouw von, Information Security management (3): the code of Practice for information security Management (BS 7799), information Management & computer Security 1998 224-225.

Solms Rossouw von, Information Security management: why standards are important, information management & computer security 1999 pp 50-57.

Solms Basies von, Rossouw von solms, The 10 Deadly Sins of Information Security Management, computer & security (2004) 23, 371-376

Toval Ambrosio, Joaquin Nicolas, Begona Moros, and Fernando Garcia, Requirement Reuse for Improving Information Systems Security: A Practitioner's Approach, Requirements Engineering, 2002 pp 205-219.

## Books:

Marshall D. Abrams, Sushil Jajodia and Harold J. Podell, *Information security; an integrated collection of Essays*, IEEE computer Society 1995

Finne Thomas, A Decision Support System for improving Information Security, Institute for Advanced Management Systems Research Åbo Akademi University, 1998 pp80-83 and pp 50-56.

IMD, Institute for Management Development, the competitiveness yearbook, 2005.

## Web sites:

- <http://www.bsi-global.com/Global/bs7799.xalter> [BS 7799]
- <http://www.isaca.org/> (COBIT)
- <http://www.theiia.org> (GASSP)
- [www.cia.gov](http://www.cia.gov)
- [www.e.finland.fi](http://www.e.finland.fi)
- [www.ficora.fi](http://www.ficora.fi)
- [www.tietoyhteiskuntaohjelma.fi](http://www.tietoyhteiskuntaohjelma.fi)
- [www.intaj.net](http://www.intaj.net)

## Appendix A

### A survey on the success factors associated with Information Security Management

#### Definition

**Information Security Management:** is the management activities used for establishing and maintaining the information security environment, including all the processes and procedures in the context of the information security environment.

#### Background Information

- Q1: **How many employees are currently working within your company? .....**
- Q2: **Does your organization have a separate Information Security Management (ISM) Department?**  
 Yes (please go to question four)     No
- Q3: **Which department manages the Information Security Management (ISM) issues?**  
 IT department     Other department    .....
- Q4: **For how long time have you been involved with Information security assignments?**  
 \_\_\_\_\_years

#### 1- Top Management Support

- Q1: **Is managing information security in your organization part of overall corporate strategy?**  
 Yes     No
- Q2: **How often is Top Management involved in reviewing and, subsequently, approving the Information Security Management (ISM) plans?**  
 Never     Sometime     Usually     Always     N/A
- Q3: **How important is the support received from Top Management for the success of managing the Information Security?**  
 Not important     Weakly important     Important

- Extremely important       N/A

## **2- Information Security Policy (ISP)**

**Q1: Does your organization have a formal Information Security Policy?**

- Yes    No

**Q2: How important is the information security policy for managing information security in your organization?**

- Not important       Weakly important       Important  
 Extremely important       N/A

**Q3: Do you agree that sufficient support from the end-users is critical to the successful implementation of the Information Security policy?**

- Don't Agree       Weakly Agree       Agree       Strongly agree  
 N/A

## **3- Job responsibilities**

**Q1: Do you agree that managing information security is everyone's job?**

- Don't Agree       weakly Agree       Agree  
 Strongly agree       N/A

**Q2: Defining the information security responsibilities in advance for each job important for the success of managing the Information security?**

- Not important       Weakly important       Important  
 Extremely important       N/A

## **4- The Motivation of the Employees**

**Q1: How important is the motivation of the employees for the success of managing the information security?**

- Not important       Weakly important       Important  
 Extremely important       N/A

**Q2: Do you agree that such a reward or appreciation system would increase the motivational level among the employees and they would become more security conscious?**

- Don't Agree       weakly Agree       Agree  
 strongly agree       N/A

**Q3: Is there any reward or appreciation system in your organization for those who perform well on Information Security Management (ISM)?**

Yes     No

### **5: Awareness and Training programs**

**Q1: How important are awareness and training programs for the successful management Information Security?**

Not important     Weakly important     Important  
 Extremely important     N/A

**Q2: Has your organization implemented any Information security awareness and training program?**

Yes     No (please go to first question of the next section)

**Q3: Does your organization manage the awareness and training program without the help of outside organizations?**

Never     Sometime     Usually     Always     N/A

### **6- Compliance with International Standards and guidelines:**

**Q1: How important is the compliance with International Standards of Information Security for the overall success of Information Security Management (ISM) in your organization?**

Not important     Weakly important     Important  
 Extremely important     N/A

**Q2: Do you make use of international information security standards for the management of information security in your organization?**

Yes     No (go to first Question of the next section)

**Q3: Do you agree that by adopting Information Security International Standards your company gains a competitive advantage over competitors?**

Don't Agree     Weakly Agree     Agree     Strongly agree  
 N/A

### **7- Need for External Experts and Advisors**

**Q1: Does your organization use the services of any external parties for managing Information Security in your organization?**

Yes     No

**Q2: Do you believe the use of consultants and external advisors play a part in the success of managing your organizations Information Security?**

- Not important       Weakly important       Important  
 Extremely important       N/A

**Q3: Does your company use the services of recruitment agencies in order to hire and contract with information security experts?**

- Never       Sometime       Usually       Always       N/A

**8- Comments**

## Appendix B

**Table (5-6)**

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5,239 <sup>b</sup>	1	,022		
Continuity Correction <sup>a</sup>	3,996	1	,046		
Likelihood Ratio	5,339	1	,021		
Fisher's Exact Test				,041	,022
Linear-by-Linear Association	5,147	1	,023		
N of Valid Cases	57				

a. Computed only for a 2x2 table

b. 0 cells (.0%) have expected count less than 5. The minimum expected count is 8,05.

**Table (5-7)**

### Group (Finland - Jordan ) \* (important of the ISP Factor) Crosstabulation

			Information Security Policy (ISP)				Total
			Not Important	Weakly Important	Important	Extremely Important	
Group	Finland	Count	2	1	22	5	30
		Expected Count	1.1 <sup>a</sup>	1.1	18.9	8.9	30.0
		% within Group	6.7%	3.3%	73.3%	16.7%	100%
		% within (ISP)	100.0%	50.0%	61.1%	29.4%	52.6%
		% of Total	3.5%	1.8%	38.6%	8.8%	52.6%
Jordan	Count	0	1	14	12	27	
	Expected Count	.9	.9	17.1	8.1	27.0	
	% within Group	.0%	3.7%	51.9%	44.4%	100%	
	% within (ISP)	.0%	50.0%	38.9%	70.6%	47.4%	
	% of Total	.0%	1.8%	24.6%	21.1%	47.4%	
Total	Count	2	2	36	17	57	
	Expected Count	2.0	2.0	36.0	17.0	57.0	
	% within Group	3.5%	3.5%	63.2%	29.8%	100%	
	% within (ISP)	100.0%	100.0%	100.0%	100.0%	100%	
	% of Total	3.5%	3.5%	63.2%	29.8%	100%	

a. Red highlighted cells that have expected count less than 5, are combined with relative cells in other columns in order to run the Chi-Square test.

**Table (5-8)**

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4,487 <sup>b</sup>	1	,034		
Continuity Correction <sup>a</sup>	3,319	1	,068		
Likelihood Ratio	4,547	1	,033		
Fisher's Exact Test				,043	,034
Linear-by-Linear Association	4,407	1	,036		
N of Valid Cases	56				

a. Computed only for a 2x2 table

b. 0 cells (,0%) have expected count less than 5. The minimum expected count is 7,43.

**Table (5-9)**

**Group (Finland - Jordan)\* (important the Job Responsibilities) Crosstabulation**

			Job Responsibility (Job Res.)				Total
			Not Important	Weakly Important	Important	Extremely Important	
Group	Finland	Count	2	3	20	5	30
		Expected Count	1,6 <sup>a</sup>	2,1	17,7	8,6	30,0
		% within Group	6,7%	10,0%	66,7%	16,7%	100%
		% within Job Res.	66,7%	75,0%	60,6%	31,3%	53,6%
		% of Total	3,6%	5,4%	35,7%	8,9%	53,6%
	Jordan	Count	1	1	13	11	26
		Expected Count	1,4	1,9	15,3	7,4	26,0
		% within Group	3,8%	3,8%	50,0%	42,3%	100%
		% within Job Res.	33,3%	25,0%	39,4%	68,8%	46,4%
		% of Total	1,8%	1,8%	23,2%	19,6%	46,4%
Total	Count	3	4	33	16	56	
	Expected Count	3,0	4,0	33,0	16,0	56,0	
	% within Group	5,4%	7,1%	58,9%	28,6%	100%	
	% within Job Res.	100,0%	100,0%	100,0%	100,0%	100%	
	% of Total	5,4%	7,1%	58,9%	28,6%	100%	

a. Red highlighted cells that have expected count less than 5, are combined with relative cells in other columns in order to run the Chi-Square test.

**Table (5-10)**

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.565 <sup>a</sup>	2	.277
Likelihood Ratio	2.648	2	.266
Linear-by-Linear Association	1.516	1	.218
N of Valid Cases	56		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 5.30.

**Table (5-11)**

**Group (Finland - Jordan) \* (The Motivation of the Employees) Crosstabulation**

			The Motivaiton of the Employees (ME)				Total
			Not Important	Weakly Important	Important	Extremely important	
Group	Finland	Count	8	1	10	10	29
		Expected Count	5.7	2.1 <sup>a</sup>	10.9	10.4	29.0
		% within Group	27.6%	3.4%	34.5%	34.5%	100.0%
		% within (ME)	72.7%	25.0%	47.6%	50.0%	51.8%
		% of Total	14.3%	1.8%	17.9%	17.9%	51.8%
Jordan	Count	3	3	11	10	27	
	Expected Count	5.3	1.9	10.1	9.6	27.0	
	% within Group	11.1%	11.1%	40.7%	37.0%	100.0%	
	% within (ME)	27.3%	75.0%	52.4%	50.0%	48.2%	
	% of Total	5.4%	5.4%	19.6%	17.9%	48.2%	
Total	Count	11	4	21	20	56	
	Expected Count	11.0	4.0	21.0	20.0	56.0	
	% within Group	19.6%	7.1%	37.5%	35.7%	100.0%	
	% within (ME)	100.0%	100.0%	100.0%	100.0%	100.0%	
	% of Total	19.6%	7.1%	37.5%	35.7%	100.0%	

a. Red highlighted cells that have expected count less than 5, are combined with relative cells in other columns in order to run the Chi-Square test.

**Table (5-12)**

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.686 <sup>b</sup>	1	.408		
Continuity Correction <sup>a</sup>	.305	1	.581		
Likelihood Ratio	.687	1	.407		
Fisher's Exact Test				.582	.291
Linear-by-Linear Association	.673	1	.412		
N of Valid Cases	56				

a. Computed only for a 2x2 table

b. 0 cells (.0%) have expected count less than 5. The minimum expected count is 10.50.

**Table (5-13)**

**Group (Finland - Jordan) \* (The Awareness and Training Programs) Crosstabulation**

			Awareness and Training Programs (ATP)				Total
			Not Important	Weakly Important	Important	Extremely Important	
Group	Finland	Count	1	2	16	9	28
		Expected Count	1.0 <sup>a</sup>	1.0	15.5	10.5	28.0
		% within Group	3.6%	7.1%	57.1%	32.1%	100.0%
		% within (ATP)	50.0%	100.0%	51.6%	42.9%	50.0%
		% of Total	1.8%	3.6%	28.6%	16.1%	50.0%
Jordan	Jordan	Count	1	0	15	12	28
		Expected Count	1.0	1.0	15.5	10.5	28.0
		% within Group	3.6%	.0%	53.6%	42.9%	100.0%
		% within (ATP)	50.0%	.0%	48.4%	57.1%	50.0%
		% of Total	1.8%	.0%	26.8%	21.4%	50.0%
Total	Total	Count	2	2	31	21	56
		Expected Count	2.0	2.0	31.0	21.0	56.0
		% within Group	3.6%	3.6%	55.4%	37.5%	100.0%
		% within (ATP)	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	3.6%	3.6%	55.4%	37.5%	100.0%

a. Red highlighted cells that have expected count less than 5, are combined with relative cells in other columns in order to run the Chi-Square test.

**Table (5-14)**

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.961 <sup>a</sup>	2	.007
Likelihood Ratio	10.376	2	.006
Linear-by-Linear Association	3.026	1	.082
N of Valid Cases	56		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 5.30.

**Table (5-15)**

**Group (Fin - Jo) \* (Compliance with Information Security international Standards) Crosstabulation**

			Compliance with Information Security International Standards (CISIS)				Total
			Not Important	Weakly Important	Important	Extremely important	
Group	Finland	Count	1	13	11	4	29
		Expected Count	.5 <sup>a</sup>	7.3	16.6	4.7	29.0
		% within Group	3.4%	44.8%	37.9%	13.8%	100%
		% within (CISIS)	100.0%	92.9%	34.4%	44.4%	51.8%
		% of Total	1.8%	23.2%	19.6%	7.1%	51.8%
	Jordan	Count	0	1	21	5	27
		Expected Count	.5	6.8	15.4	4.3	27.0
		% within Group	.0%	3.7%	77.8%	18.5%	100%
		% within (CISIS)	.0%	7.1%	65.6%	55.6%	48.2%
		% of Total	.0%	1.8%	37.5%	8.9%	48.2%
Total	Count	1	14	32	9	56	
	Expected Count	1.0	14.0	32.0	9.0	56.0	
	% within Group	1.8%	25.0%	57.1%	16.1%	100%	
	% within (CISIS)	100.0%	100.0%	100.0%	100.0%	100%	
	% of Total	1.8%	25.0%	57.1%	16.1%	100%	

a. Red highlighted that have expected count less than 5 are combined with relative cells in other columns in order to run the Chi-Square test.

**Table (5-16)**

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2.627 <sup>b</sup>	1	.105		
Continuity Correction <sup>a</sup>	1.811	1	.178		
Likelihood Ratio	2.666	1	.103		
Fisher's Exact Test				.169	.089
Linear-by-Linear Association	2.581	1	.108		
N of Valid Cases	57				

a. Computed only for a 2x2 table

b. 0 cells (.0%) have expected count less than 5. The minimum expected count is 9.95.

**Table (5-17)**

**Group (Fin - Jo) \* (Use the Services of the External Information Security Experts) Crosstabulation**

			Need for External Information Security Experts (NEISE)				Total
			Not important	Weakly Important	Important	Extremely Important	
Group	Finland	Count	3	11	15	1	30
		Expected Count	2.1 <sup>a</sup>	8.9	18.4	.5	30.0
		% within Group	10.0%	36.7%	50.0%	3.3%	100%
		% within (NEISE)	75.0%	64.7%	42.9%	100.0%	52.6%
		% of Total	5.3%	19.3%	26.3%	1.8%	52.6%
Jordan	Jordan	Count	1	6	20	0	27
		Expected Count	1.9	8.1	16.6	.5	27.0
		% within Group	3.7%	22.2%	74.1%	.0%	100%
		% within (NEISE)	25.0%	35.3%	57.1%	.0%	47.4%
		% of Total	1.8%	10.5%	35.1%	.0%	47.4%
Total	Total	Count	4	17	35	1	57
		Expected Count	4.0	17.0	35.0	1.0	57.0
		% within Group	7.0%	29.8%	61.4%	1.8%	100%
		% within (NEISE)	100.0%	100.0%	100.0%	100.0%	100%
		% of Total	7.0%	29.8%	61.4%	1.8%	100%

a. Red highlighted that have expected count less than 5 are combined with relative cells in other columns in order to run the Chi-Square test

## Appendix C

**Table 5-22**

**is the ISM part of Corporate strategies (Yes - No) \* (Importance of the TMS) Crosstabulation**

			Importance of the Top Management support (TMS)				Total
			Not Important	Weakly Important	Important	Extremely Important	
<b>Is ISM part of the Corporate Strategies</b>	Yes	Count	1	1	27	19	48
		Expected Count	.9	.9	26.6	19.7	48.0
		% within (is ISM part of Corporate Strategies)	2.1%	2.1%	56.3%	39.6%	100%
		% within Importance of the TMS	100.0%	100.0%	87.1%	82.6%	85.7%
		% of Total	1.8%	1.8%	48.2%	33.9%	<b>85.7%</b>
	No	Count	0	0	4	4	8
		Expected Count	.1	.1	4.4	3.3	8.0
		% within (is ISM part of Corporate Strategies)	.0%	.0%	50.0%	50.0%	100%
		% within Importance of the TMS	.0%	.0%	12.9%	17.4%	14.3%
		% of Total	.0%	.0%	7.1%	7.1%	14.3%
Total	Count	1	1	31	23	56	
	Expected Count	1.0	1.0	31.0	23.0	56.0	
	% within (is ISM part of Corporate Strategies)	1.8%	1.8%	55.4%	41.1%	100%	
	% within Importance of the TMS	100.0%	100.0%	100.0%	100.0%	100%	
	% of Total	1.8%	1.8%	55.4%	41.1%	100%	

**Table 5-23**

**Availability of ISP \* (Importance of the ISP) Crosstabulation**

			Importance of the ISP				Total
			Not Important	Weakly Important	Important	Extremely Important	
<b>Availability of ISP</b>	Yes	Count	1	1	31	14	47
		Expected Count	1.6	1.6	29.7	14.0	47.0
		% within Availability of ISP	2.1%	2.1%	66.0%	29.8%	100%
		% within Importance of ISP	50.0%	50.0%	86.1%	82.4%	82.5%
		% of Total	1.8%	1.8%	54.4%	24.6%	82.5%
No		Count	1	1	5	3	10
		Expected Count	.4	.4	6.3	3.0	10.0
		% within Availability of ISP	10.0%	10.0%	50.0%	30.0%	100%
		% within Importance of ISP	50.0%	50.0%	13.9%	17.6%	17.5%
		% of Total	1.8%	1.8%	8.8%	5.3%	17.5%
Total		Count	2	2	36	17	57
		Expected Count	2.0	2.0	36.0	17.0	57.0
		% within Availability of ISP	3.5%	3.5%	63.2%	29.8%	100%
		% within Importance of ISP	100.0%	100.0%	100.0%	100.0%	100%
		% of Total	3.5%	3.5%	63.2%	29.8%	100%

**Table 5-24**

**Availability of the Awareness and Training Programs \* (Importance of the Awareness and Training Programs)  
Crosstabulation**

			Importance of the Awareness and Training Programs (A&TP)				Total
			Not Important	Weakly Important	Important	Extremely Important	
<b>Availability of the Awareness and Training programs</b>	Yes	Count	1	0	15	17	33
		Expected Count	1.2	1.2	18.3	12.4	33.0
		% within Availability of A & T programs	3.0%	.0%	45.5%	51.5%	100.0%
		% within Importance of A & T programs	50.0%	.0%	48.4%	81.0%	58.9%
		% of Total	1.8%	.0%	26.8%	30.4%	58.9%
	No	Count	1	2	16	4	23
		Expected Count	.8	.8	12.7	8.6	23.0
		% within Availability of A & T programs	4.3%	8.7%	69.6%	17.4%	100.0%
		% within Importance of A & T programs	50.0%	100.0%	51.6%	19.0%	41.1%
		% of Total	1.8%	3.6%	<b>28.6%</b>	<b>7.1%</b>	<b>41.1%</b>
Total	Count	2	2	31	21	56	
	Expected Count	2.0	2.0	31.0	21.0	56.0	
	% within Availability of A & T programs	3.6%	3.6%	55.4%	37.5%	100.0%	
	% within Importance of A & T programs	100.0%	100.0%	100.0%	100.0%	100.0%	
	% of Total	3.6%	3.6%	55.4%	37.5%	100.0%	

**Table 5-25**

**Information Security International Standards implementation \* (importance of these Standards) Crosstabulation**

		Importance of the Information Security International Standards (ISIS)				Total	
		Not Important	Weakly Important	Important	Extremely important		
<b>Implementing or the ISIS</b>	Yes	Count	0	6	20	6	32
	Expected Count	.6	8.0	18.9	4.6	32.0	
	% within Implementing of the ISIS	.0%	18.8%	62.5%	18.8%	100.0%	
	% within importance of ISIS	.0%	42.9%	60.6%	75.0%	57.1%	
	% of Total	.0%	10.7%	35.7%	10.7%	57.1%	
	No	Count	1	8	13	2	24
	Expected Count	.4	6.0	14.1	3.4	24.0	
	% within Implementing of the ISIS	4.2%	33.3%	54.2%	8.3%	100.0%	
	% within importance of ISIS	100.0%	57.1%	39.4%	25.0%	42.9%	
	% of Total	1.8%	<b>14.3%</b>	<b>23.2%</b>	<b>3.6%</b>	42.9%	
<b>Total</b>	Count	1	14	33	8	56	
	Expected Count	1.0	14.0	33.0	8.0	56.0	
	% within Implementing of the ISIS	1.8%	25.0%	58.9%	14.3%	100.0%	
	% within importance of ISIS	100.0%	100.0%	100.0%	100.0%	100.0%	
	% of Total	1.8%	25.0%	58.9%	14.3%	100.0%	

**Table 5-26**

**Using the Services of the External Information Security advisors\* (Importance of using these Services Crosstabulation)**

			Importance of Using the Services of the External Information Security Advisors (USISA)				Total
			Not important	Weakly Important	Important	Extremely Important	
<b>Using the Services of the External Information Security Advisors (USISA)</b>	Yes	Count	1	9	17	1	28
		Expected Count	2.0	8.4	17.2	.5	28.0
		% within USISA	3.6%	32.1%	60.7%	3.6%	100.0%
		% within Importance of USISA	25.0%	52.9%	48.6%	100.0%	49.1%
		% of Total	1.8%	15.8%	29.8%	1.8%	49.1%
	No	Count	3	8	18	0	29
		Expected Count	2.0	8.6	17.8	.5	29.0
		% within USISA	10.3%	27.6%	62.1%	.0%	100.0%
		% within Importance of USISA	75.0%	47.1%	51.4%	.0%	50.9%
		% of Total	5.3%	<b>14.0%</b>	<b>31.6%</b>	.0%	50.9%
Total	Count	4	17	35	1	57	
	Expected Count	4.0	17.0	35.0	1.0	57.0	
	% within USISA	7.0%	29.8%	61.4%	1.8%	100.0%	
	% within Importance of USISA	100.0%	100.0%	100.0%	100.0%	100.0%	
	% of Total	7.0%	29.8%	61.4%	1.8%	100.0%	