Analytical Study of Gaps between ISM Teaching and Practice in Pakistan

By

Hafiza Rabbia Anwar

00000172704

Supervisor

Dr. Hasan Tahir

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Security (MS IS)

In

School of Electrical Engineering and Computer Science,

National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(October 2019)

Approval

It is certified that the contents and form of the thesis entitled "Analytical Study of Gaps between ISM Teaching and Practice in Pakistan" submitted by Hafiza Rabbia Anwar has been found satisfactory for the requirement of the degree.

.

Advisor: Dr. Hasan Tahir

Signature: _____

Date: _____

Committee Member 1:

Ms. Haleemah Zia

Signature: _____

Date: _____

Committee Member 2:

Dr. Abdul Ghafoor Abbasi

Signature: _____

Date: _____

Committee Member 3:

Dr. Mehdi Hussain

Signature: _____

Date: _____

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by Ms. Hafiza Rabbia Anwar, (Registration No 172704), of School of Electrical Engineering and Computer Science (SEECS) has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: Dr. Hasan Tahir

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

Certificate of Originality

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: Hafiza Rabbia Anwar

Signature: _____

Acknowledgment

I thank Allah for giving me the strength to make this little effort reach fruition and for constant reminder that His plans are better than my dreams.

I am greatly obliged to my family for their unconditional love, continuous support, encouragement and prayers in all my endeavors. My deepest gratitude to my parents for bringing the confidence in me to reach for the stars and chase my dreams.

I am grateful to my Supervisor, Dr. Hasan Tahir for his patient guidance, encouragement and advice to complete my thesis and for giving me numerous opportunities to learn and grow and Ms. Haleemah Zia for co-supervising this thesis.

I am also thankful to Dr. Abdul Ghafoor Abbasi and Dr. Mehdi Hussain for being on my thesis guidance and evaluation committee.

I am overwhelmed to acknowledge my depth to all those who have helped me to put these ideas into something concrete, specially Mr. Muhammad Azzam Sharif for helping me in conducting survey and Ms. Tanzila Akmal for her guidance regarding survey analysis.

Last, but not the least, I thank my all friends for making NUST a home.

Table of Contents

List of Abbreviation

IS	Information Security
ISM	Information Security Management
SPSS	Statistical Package for Social Sciences
SEECS	School of Electrical Engineering and Computer Sciences
NUST	National University of Sciences and Technology
RM	Risk Management
RA	Risk Assessment
ISRM	Information Security Risk Management
ISRA	Information Security Risk Assessment
BCP	Business Continuity Planning
DRP	Disaster Recovery Planning
COBIT	Control Objectives for Information and Related Technologies

List of Tables

List of Figures

Related Publication

Anwar, R., Zia, H., Tahir, H., Tahir, S., Hussain, M., "Analytical Study of Gaps between ISM Teachings and Practices in Pakistan". To be submitted.

Abstract

Information security consists of technical views for securing the Information like security protocols, cryptographic tools, firewalls, intrusion detection and protection systems as well as information security management methods and tools like controls and policies at organizations, risk management policies and incident management etc. Managing information security is more critical. In recent years, advances in information security management (ISM) are rapid at organizational level. A gap exists in what is being taught in educational institutes and being practiced in industry in ISM. There are very limited evidences and studies on how to design and teach ISM in educational institutes. It is also not clear that which factors are necessary for ISM curricula designing and whether all factors are equally important or which factors are not that important.

This research examines the gaps in teachings and industry practices of ISM in Pakistan. Gap analysis was done on the current information security Management course outline of SEECS- NUST Islamabad, Pakistan. To analyze this gap and to examine the topic selection for the curricula being taught, a survey has been conducted from information security Management personnel from different organizations of Pakistan.

Keywords: *Information Security, Information Security Management, gap analysis, curricula designing, Social Science Data Analysis tool, ISM Practitioners.*

Introduction

This chapter presents the facts and figures that explains the importance of information security management (ISM) both in IT industry and academia. This section defines the challenges, problem and solution statement for this research and key contribution. The outline of all other chapters also included in this section

It has been observed that there can be a significant difference in what is being taught in information security Management (ISM) and that being practiced in organizations[1]. Organizations need to maintain the safety of information assets and to handle them securely [2]. On the other hand, universities are accountable for producing the graduates who are equipped with the skills to perform information security tasks[3]. Thus, graduates must have basic skill-set required to meet the information security (IS) operations performed in organizations. Most IS graduates only possess theoretical knowledge and have no idea of actual implementations[1]. As a result, they face problems in organizations where ISM is rigorously practiced. Most universities take information security as technology-oriented e.g. cryptography, network security, artificial intelligence and other technical subjects but information security Management is equally important for any organization[4].

This implies that a need exists to design a curriculum that equips students with skills needed to manage Information at organizational level because information management requires a broad set of formal, informal and technical skills[4]. Graduates should have ability to align information security controls and principles to real-time organizational scenarios. To design such information security management curricula, universities must be aware of industry needs and how this aligns with course content and curricula. Despite the significant role of information security management teachings and practices and the gap that exists between them, little pragmatic investigations are reported in the scholarly literature to address the aspects that are necessary to align the ISM teachings with industry practices. We tried to address this gap by pointing out which topics should be added in ISM curricula and, how current topics in course outline can be improved.

In this study, a survey has been conducted among information security practitioners to determine where graduates lack in implementing information security management knowledge in organizations and how it can be improved by analyzing the results with the help of social sciences data analysis tool (SPSS)[5][6]. Based on obtained results we tried to observe where exactly graduates lack, either the selection of topics being taught is not appropriate or the level of knowledge imparted by teaching those topics is not providing the required skills. We choose information security practitioners for the survey because they observe graduates closely at their jobs. This study was needed because of an evolution of information security industry with a sprouting threat environment in Pakistan. In mid of October 2018 Pakistan's financial organization was hit by the major cyber security attack in country's history [7][8][9]. This attack was on

user accounts of renowned bank in Pakistan that costs them Rs.2.6 million. While the amount was rather uncertain, the incident alerts regarding information security measures within the financial division, revealing further vulnerabilities [10]. In order to guard against these attacks proper information security management knowledge is needed, and educational institutes are responsible to provide the required knowledge to the students perusing information security degree. Universities needs to design proper policies and work on the factors that are important in curricula designing. To address the gaps between teachings and practices of ISM in Pakistan we have suggested few improvements that can be helpful in ISM curricula designing for future and these findings are also useful for improvement of current teaching techniques and to provide an aid for researchers and IS practitioners to further bridge this gap in literature and contribute to build a rich foundation for further research in this area.

1.1. Challenge

Information security management (ISM) is trending in Pakistan rapidly and at the same time information security breaches also increasing in Pakistan. This creates a challenging situation for both ISM practitioners and instructors. Practitioners needs to design policies and procedures to create secure information security environment in Pakistan and ISM instructors needs to align their teaching materials to currently adopted ISM trends[4][11][3].

The main challenge in conducting this research was that there is very limited scholarly literature available on this topic and no study had been conducted in Pakistan. The targeted group pf people were all information security practitioners from multiple organizations, approaching them was also a big challenge. The survey analysis was done by using Statistical Package for Social Sciences (SPSS) which is a social sciences tool and it was not explored before.

1.2. Problem Statement

Previous research has pointed out that a gap exists in ISM teachings and industry practices. In this study, we intend to explore whether such a gap actually exists; particularly in the context of ISM being taught at NUST-SEECS and the ISM practice in Pakistan by conducting a survey. Keeping in mind the results obtained, suggestions would be given for better curricula designing for information security management.

1.3. Solution Statement

In this study, we conducted a survey to point out these gaps in current course outline of information security management (ISM) at SEECS-NUST and also tried to provide few solutions which can be helpful in future.

1.4. Thesis Aims and Objectives

Our objective is to encompass majority of research in this field through literature of our choice. We aim to divide our work in two steps:

(1) Verify the existence of such gap in Pakistani Institutions in particular

(2) carry out a research that leads to an improved course structure for ISM, one that aligns the theory to practice.
we carried out the process with the help of interviews, questioners and their analysis.

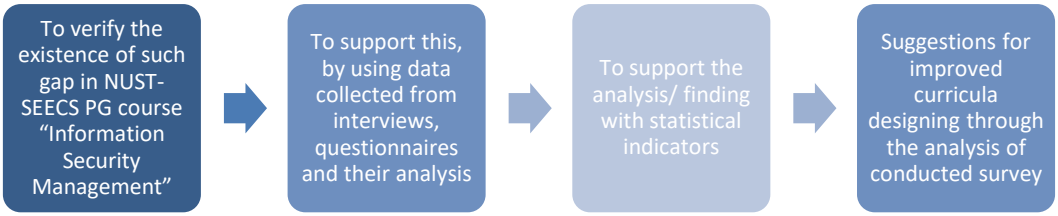

Figure 1: Objectives

1.5. Research Impact

Our proposed study analyzed the current practices of information security Management in Pakistan, it point out the gap present in industrial practices and ISM teachings in Pakistan. In the light of results obtained from a survey conducted we proposed suggestions to improve current course outline and showed that how the involvement of ISM practitioners can be used in curricula designing.

1.6. Model of Study

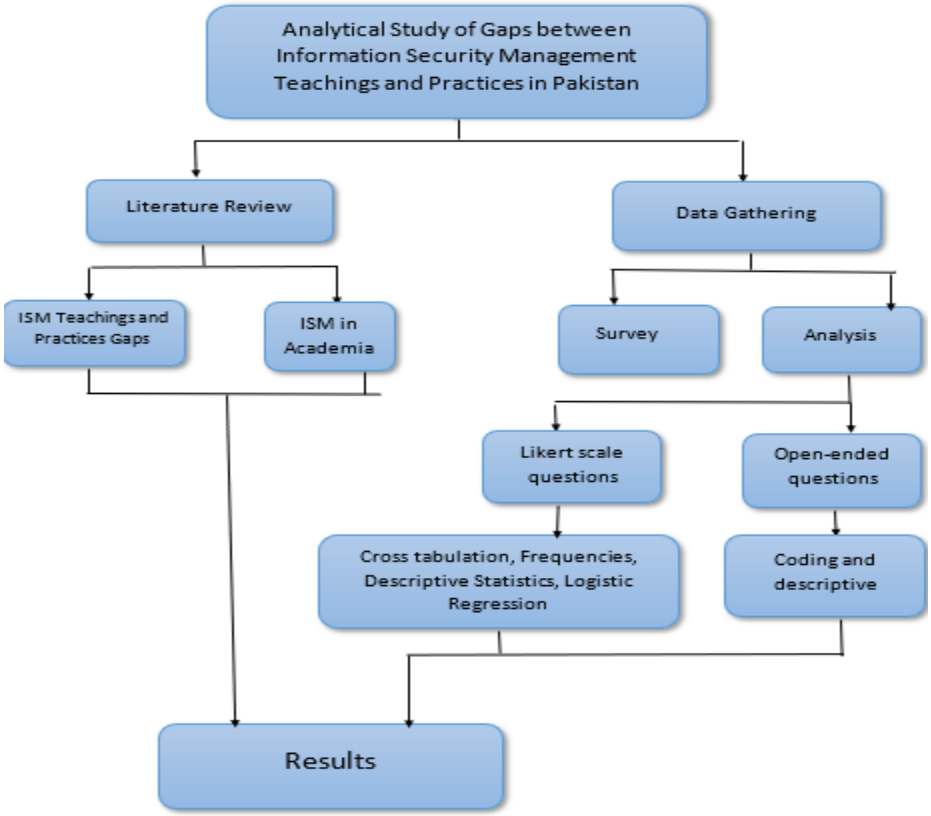

Figure 2: Model of Study

Figure 2 shows the flow of this study. This research is divided into two phases, one is literature review in which we explored related scholarly literature and the other is data gathering that was done by conducting a survey and its analysis by using SPSS tool. At the end results are obtained.

1.7. Thesis Organization

Rest of the thesis is organized in following chapters

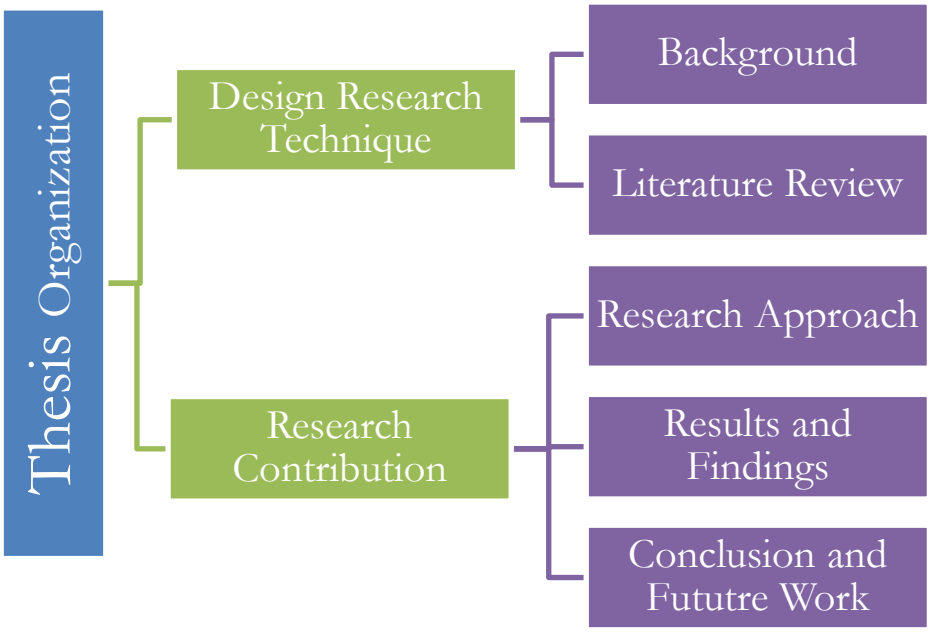

Figure 3: Thesis Organization

1.7.1. Chapter 2: Background

Chapter 2 provides overview of information security and information security management and how ISM is rapidly trending in Pakistan and how the threat environment is also getting strong accordingly. The brief overview of information security management practices is also included in this section for better understanding.

1.7.2. Chapter 3: Literature Review

This chapter explains the scholarly literature related to information security management curricula designing and teachings and ISM industry practices. The literature review section is further divided into two sections, one section covered the scholarly literature-based ISM curricula designing and ISM teaching approaches. The other section consists of literature on ISM practices in industry.

1.7.3. Chapter 4: Research Approach

This chapter defines the method adopted to do this study which elaborates how the survey is being conducted and how we determine the sample size. Survey analysis and its results are also included in this section. Each test is elaborated separately. This chapter defines the trends and outcomes we got after statistical analysis.

1.7.4. Chapter 5: Results and Findings

This chapter demonstrates the outcomes we got at the end of the survey and analysis of all the tests done with the help of SPSS tool and open-ended questions analysis techniques. This section describes the final results in a tabular form and clear and bold statements that are easy to understand the study results.

1.7.5. Chapter 6: Conclusion and Future work

This section briefly concludes this thesis and the outcomes of this study and at the end limitations in this thesis are also discussed along with suggestions on how this study can be improved more in future by later researchers.

Background

This chapter presents provides overview of information security and information security management and how ISM is rapidly trending in Pakistan and how the threat environment is also getting strong accordingly. The brief overview of information security Management practices is also included in this section for better understanding.

2.1. Information security

Information security Management is vital for any organization to securely operate[12]:

I. The critical information
II. To check the reliability of that information

Figure 4 shows information security principles [13].

Figure 4: Information Security

2.2. Information Security Management

Information security Management is vital for any organization that have any information assets that are confidential for that organization. Information security can be managed by designing policies and procedures according to organization's environment (not every policy is suitable for every organization). Organizations need well trained resources to design and implement ISM policies and procedures[14][15].

2.3. Information Security incidents in Pakistan

The noticeable information security incident occurred in Pakistan in October 2018 was identity theft in which credit card information of many users was compromised and attackers took roughly 2.6 million from user accounts. This showed the weakness of security policies in finance sector of Pakistan[7][10]. The attack was done on international payments and users are tricked to show their secure pin codes and credit card information via scam emails and calls. These attacks showed that there is no single vulnerability in Pakistan's banking sector, the whole system is highly vulnerable whether we look at users or cyber security departments of banks. All this situation shows that people are still unaware of the concept of information security in Pakistan. This is the duty of security practitioners to provide awareness to the users about online banking system and its security. Financial sector needs to invest more in their cyber security departments [16]. This links to the employee awareness towards information security and the importance of information security education provided by educational institutes.

Figure 5: IS Incidents in Pakistan

2.4. Information Security practices in organizations

Information security Management is vital for any organization to securely operate the critical information and to check the reliability of that information[3]. Universities most of the time, focuses on teaching technical aspects of information security but often lack in teaching non-technical security management skills[4]. Information security certifications are expensive hence, in a developing country like Pakistan

students and practitioners often rely on academia as their primary source of knowledge. In Pakistan, people are not much aware about the security aspects of their online data and information, so information security is still a vague concept. Only few educational institutes are offering a degree in information security and most of the curricula is technology oriented which is equally preferred by instructors and students but as discussed earlier there are multiple non-technical aspects to secure information. information security management practices in any organization broadly comprise of:

2.4.1. Information Security Risk Management (ISRM)

Protecting complex information resources from the evolving threat environment is a challenge for organizations. Organizations are recommended to follow risk management approaches to secure the information. Risk management related objectives are: risk identification, assessment, treatment and risk review [17][18]. Organizations are recommended to follow risk management objectives to treat the risks and secure the information assets from threats. Figure 6 elaborates the risk management cycle [19].

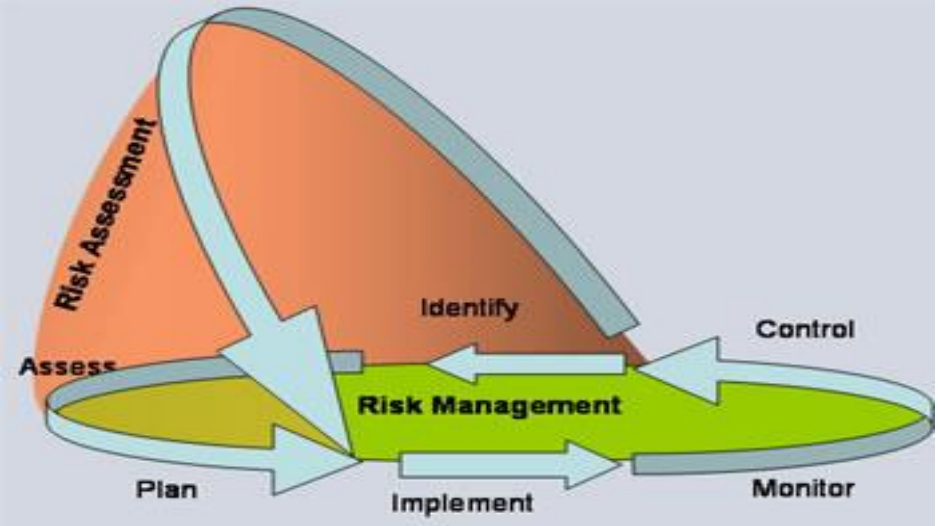

Figure 6: Risk Management

2.4.2. Information Security Risk Assessment (ISRA)

Information security risk assessment (ISRA) enables the organizations to identify the security assets, the threats and their impacts on the business. Additionally, it also identifies risk states, their consequences and likelihood of occurrence, risk treatment and cost related to that treatment. The main challenge for any organization is how to perform risk assessment effectively [20]. Organizations should perform ISRA to identify the risks and their impacts on security resources, so the risk management can be cost-effective and quick. Figure 7 shows the IT Risk Assessment cycle [21].

Figure 7: IT Risk Assessment

2.4.3. ISO standards

"Standards rise through the development of thorough descriptions of specific features of a product or service by professionals from companies and scientific institutions. They represent a consent on characteristics such as quality, security and reliability that should remain valid for prolonged period and thus are documented and get published". ISO 27001 standard is the foundation of ISO 27k series of standards which cover series of standards for information security management [22]. Organizations must align their policies to these standards, so they can meet international organizations standards. Organizations should periodically check the compliance of these standards with their organization's current practices.

2.4.4. Incident Management

It includes both reactive and pro-active approaches to handle the security incidents. Pro-active techniques are for timely detection of incident and keep the situation in control. Reactive approaches are for dealing with the incidents that are already occurred. Most organizations have incident response teams, but a holistic approach is to have incident management team to take both reactive and pro-active actions [23]. When organizations follow incident management techniques they can perform better in case of anomalies and interruption of operations.

2.4.5. Business continuity and disaster recovery

Business continuity planning (BCP) offers techniques and methods for dealing with long-standing outages and adversities. Disaster recovery planning (DRP) is for minimizing the effects of any disruption in business operations. These plans are mostly IT focused [23][24]. BCP and DRP make sure that organizational operations keep going in case of any disaster and recovery is feasible.

2.4.6. COBIT

COBIT allows the managers to manage and govern the I & T resources by a controlled set of measures to provide I & T services that provide the information essential for any organization [25]. By implementing COBIT, I & T governance standards can be followed in organization. COBIT make sure to minimize I & T related risk in an organization. Figure 8 shows the COBIT framework principles [25].

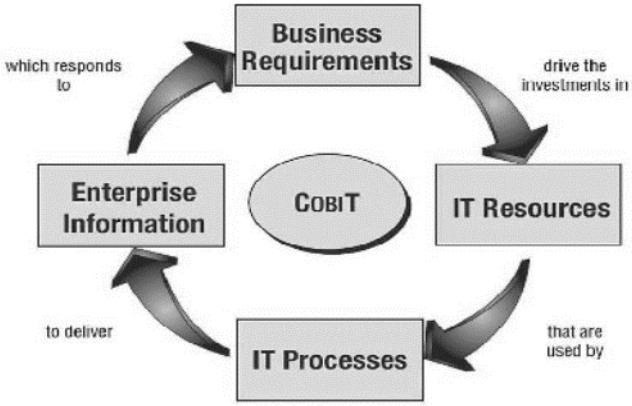

Figure 8: COBIT Framework Principle

Literature Review

This chapter includes review of existing scholarly literature to provide insight of this study. This section presents the literature breakdown and then brief overview of each section is also included.

3.1. Area of Research

In this section, we discussed the work that highlights different aspects to define the domain of information security management (ISM) and its related aspects that can be linked with better curricula designing and can be helpful in gap identification. We have found very limited and sparse literature that addresses the gaps between information security management teachings and practices. Therefore, we have consulted the literature based on ISM curricula designing and teaching and ISM practices in industry which supports us to recognize the factors that causes the gap between ISM teachings and practices and how to cope with these gaps efficiently and successfully both in academia and industry. Literature related to statistical analysis of questionnaire and test results are also included in this section.

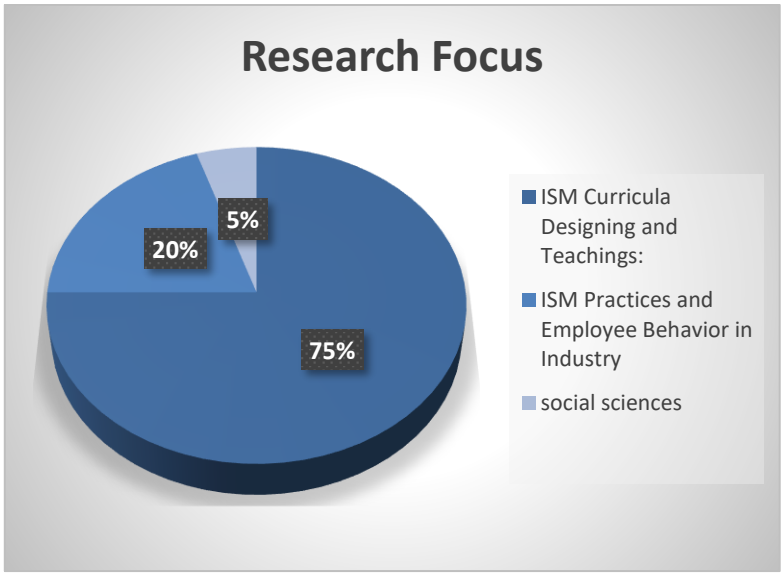

Figure 9: Research Focus

The scope and contribution of related literature is briefly described in this section:

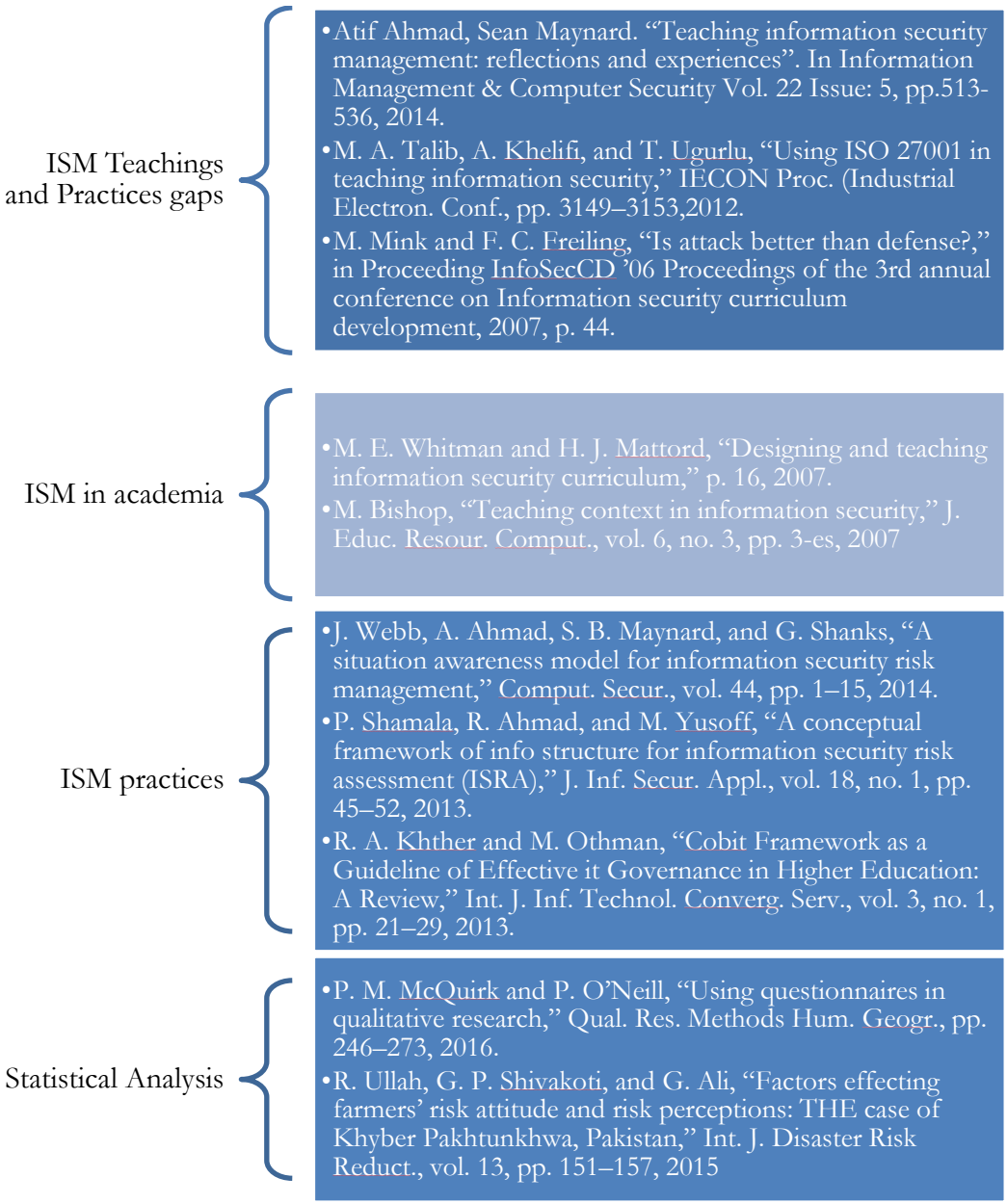

Figure 10: Literature Review Summary

3.1.1. ISM Curricula Designing and Teachings:

M. A. Talib *et al* [3], emphasis on importance of information security management at organizational level and demonstrate that universities are responsible to produce graduates that can perform information security functions to uphold the information continuously. Authors implemented the improved ISM course curricula at Zayed University UAE after interviewing alumni and students currently serving as interns in the information security industry. They found out

that there is a gap what students learning and actual practices. The proposed solution comprises of adding ISO 27001 standards guidelines in ISM course to meet international standards of practicing ISM. They have supported this approach by engaging students with organizations scenarios to get hands-on experience.

In [4] A. Ahmad *et al*, argued that the teaching curricula for information security is mainly focuses on technical areas like protocols for network security, cryptographic applications and the like. In turn, students are inadequately trained in information security management. The primary aim of authors is to design a subject that will train students for enterprise level information security management practices, allow maximum student involvement and at the end students assessment. Authors have given the reasons why technical subjects alone are not suitable for management practitioners. Authors proposed 3 main principles: "IS protects business functions, IS protects information and knowledge and lastly, information security is people's problem having technical solution" that should be considered while designing the ISM course curricula. The proposed teaching model was workable for small class size (less than 50 students).

In [26] L. Futcher *et al*, reviews the literature regarding outcome-based information security knowledge in universities of South Africa and proposed the approach in which educators can integrate information security knowledge into their learning programs. The authors argued that in universities of South Africa, information security is being taught on ad-hoc basis at undergraduate level. Although information security is important for any organization from both social and economic perspectives. To analyze the behavior regarding educator's perspective regarding the extent of information security knowledge required in CS, IT programs for undergraduates, authors conducted a survey. The results showed that information security is not adequately taught at undergraduate level. Undergraduates must know about basic information security controls and policies and their use.

In [11] M. Mink *et al*, build the motivation to design curricula on offensive techniques. information security curricula are mostly based on defensive techniques like cryptography, intrusion detection, firewall and others. No doubt these techniques are important but should be integrated with offensive information security techniques like risk management, IS policies and controls. These offensive techniques are also getting wide approval in security literature. Authors have reviewed the IT security curricula at RWTH Aachen University and found that it is defensive techniques based only. Authors did empirical study based on hypothesis "Students who received offensive information security teaching have an improved understanding of IT security than those who received defensive teaching" by applying survey technique of social sciences. Only empirical study has been done by making two different groups of students, one group is being taught offensive techniques and the other group defensive techniques. Authors

leave the experimental set-up for future and to show the results later. No clear results has been shown in this paper.

M. E. Whitman *et al* [1], discussed that unlike other information technology subjects. information security is not producing graduates with the skill set required by organizations. Most information security specialists are trained on their jobs. Authors discussed the approaches to improve curricula designing and teaching practices. They mapped positions to roles to knowledge areas of information security and defined which information security position have what roles and require what kind of knowledge. Figure 11 elaborates this mapping [1].

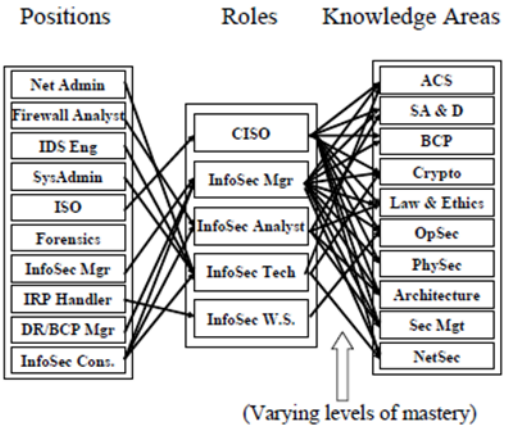

Figure 11: Mapping of Positions to Roles to Knowledge Areas

Author M. Bishop throws light on the issue that mechanisms that are suitable in one case are not suitable in other cases, so it is important to have non-technical security education because it provides more holistic view of a problem than a technical security education. Author proposed to design a course with puzzles for students and case studies from different organizations. Students enjoyed and learned a lot from this puzzle-time [27].

R. Hackney *et al*, described that using case studies as a teaching aid in IS education. Case teaching method brings real world examples into the class rooms and allow students to learn from doing actual tasks and students can experience real organizational environment. Authors also discussed the limitations of this technique by saying that occasional use of cases can make both students and teacher uncomfortable and it does not cover complete information [1].

Wu He *et al*, also suggested that use of authentic case studies while teaching information security can successfully engage students to learn about information security principles that are being applied in workflow of any organization and involvement of professionals from different organizations in curricula designing for information security is also increasing. Authors also provided two real life case studies in this publication for information security students. But the limitation of this study is the small sample size [28].

W. Alec Cram *et al*, emphasize on the importance of information security knowledge in business school because to manage the business operation and to maintain the security of critical assets one must have knowledge of information security. They proposed the course of information security comprises of technical and managerial knowledge for business studies students. This study follows the information security approaches for specific areas in U.S and proposed solution for that areas. The technique may not be workable for other areas [29].

3.1.2. ISM Practices and Employee Behavior in Industry:

Mikko Siponen *et al*, described that employees of any organization proved to be potential threat to the security of that organization if they do not comply with information security policies. Authors developed multi-theory model to check the employee observance of information security policies of organization and test this model on 669 employees of an organization in Finland. They found out that employee intentions to comply with information security policies is an important factor to actual compliance with these policies. Hands on training sessions and security education can prove helpful for employees. This study only covered one organization and there is no reliability check for questionnaire (one employee can submit multiple responses) [30].

Teodor Sommestad *et al*, argued that employee willingness to adopt information security safety measures is imperative to their own and their organization's information security. This publication tests the "protection motivation theory" which can be used for multiple reasons and one of them is to check information security behavior. This theory has been tested by authors through 28 different surveys. The authors provide guidelines and suggestions to use this theory to test and improve information security behavior among employees [31].

Heru Susanto *et al*, described that there is no single formula to get 100% information security so there is a need to have a set multiple security standard to get adequate level of security. This publication contains various standards and their comparison to design best information security policies for organization. Authors also recommended that further research is required to refine the standard ISO (27001) [32].

Zahoor Ahmad Soomro *et al*, discussed that with the increasing information security trends in business and it also increased the risk and strengthen the threat environment. Previous research showed that information security was taken as technical studies but now researchers are somehow focusing on managerial aspects of information security. This publication comprises of holistic literature review provided for information security managers to design policies and procedures for their organizations. Authors claimed that their research can be helpful for managers for better performance of their roles [33].

Hyeun-Suk Rhee *et al*, argued that increasing threats of information security management in organizations are directly related to inadequate managerial level awareness of ISM and threat environment. Authors have tested the hypothesis based on optimistic biased theory. The results showed that information security managers have optimistic bias (to think that this risk might not affect us as it affect others) [12].

While studying the relevant literature, it became obvious that there are no previous studies that connect Information security practitioners with the information security management curricula of Pakistan. Therefore, detailed study of gaps between ISM teachings and practices in Pakistan will provide much needed insight.

Research Approach

This chapter describes the approach we followed for this study. How the sample size is determined, and the tool is being selected for analysis and results.

This research project is in its early stages and little information is provided in scholarly literature about what factors causing these gaps and what are the essentials to design and teach information security management, we have selected a suitable approach to identify the gaps between teachings and practices of ISM. We adopted the approach commonly used in social sciences which is data gathering relevant to curricula designing and teaching approaches currently being used by a SEECS-NUST Islamabad, Pakistan and how it can be improved. We did not test any theory that is already present rather our intention was to develop a guideline that proves to be helpful for better curricula designing and after that we suggest few ways in the light of our findings that should be followed in order to bridge the gap between ISM teachings and practices.

4.1. Case Description:

To do in depth analysis to find out the gaps between ISM teachings and practices in Pakistan, a survey has been conducted from information security practitioners belongs to different organizations of Islamabad, Pakistan and obtained their views on current course outline of information security management being taught in SEECS-NUST to students of master's in information security program. The selected educational institute has one of the oldest running postgraduate security program in Pakistan and it is a large and highly reputed university which produce in between 50 to 100 information security graduates per annum and these graduates are working in all over the Pakistan in government, federal and non-government sectors and also many are working abroad . The survey has been taken from information Security employees of different organizations (1 government and 15 non-government) involved in performing ISM functions for securing information assets within the organization or perform IT audits for other organizations as an external auditor. The information security industry has been chosen as it is able to provide the most relevant feedback about fresh graduates. information security practitioners closely observe their performance and skills. To perform this survey multiple rounds of two activities has been done. Firstly, the questionnaires filled out by selected IS practitioners consist of IS consultants, managers, analysts, engineers, assessment experts and research assistants. Secondly, open group discussion has been done with respondents. Multiple tests have been done to check the reliability and usability of the data obtained by the survey conducted. To perform these tests we have used SPSS which is the tool used by the students and researchers of social sciences.

4.2. Data collection and analysis:

Data analysis was done as described below:

4.2.1. Questionnaire

The questionnaire was based on the course outline currently being taught in SEECS-NUST Islamabad, Pakistan. We took each topic from course outline and asked 3 questions about each of the topic. The questions were as follows:

i) Do you think teaching this topic is essential and it does help prepare the students for the industry?
ii) Do you think the knowledge and skills imparted from this topic meet your organization's standards?
iii) Are the graduates equipped with skills and attitude for applying the knowledge in the practical field?

Respondents had to answer these questions in Likert scale which were then evaluated by multiple tests in SPSS and at the end respondents had to answer 3 open-ended questions which were as follows:

i) How do you think training in these topics can be improved?
ii) At what level should graduates be trained in these topics?
iii) What new topics, do you think should be added to the course outline?
These open-ended questions than evaluated by manual coding method.

Figure 12: Questionnaire

4.2.2. Data Collection

Collecting the data was the most difficult part of the whole process because information security practitioners were few and far between in most of the organizations and they have multiple duties to perform. Time management was the main issue for the people filling the questionnaires because it was covering the complete course outline. The questionnaire starts with demographic information like respondent name, department and organization's name and after questions related to improvement in each topic of the course outline and at the end suggestions for overall

curricula. Both open-ended and close ended questions were included within this questionnaire. First, we determined the sample size (how many questionnaires should be filled?) by the help of the following formula [34]:

$$n = \frac{N}{1 + Ne^2} \quad where, n = sample\ size$$

$$N = total\ number\ of\ IS\ employees\ in\ targeted\ organizations$$

$$e = precision\ which\ is\ set\ at\ 15\%\ (0.15) \quad [34]$$

total number of employees are approximately 90 so we need to get responses from 30 people and we have got 33 responses in total. 15% precision means we are 85% sure about sample size we took.

4.2.3. SPSS (Statistical Package for Social Sciences)

The data analysis was done on the tool called SPSS (Statistical Package for Social Sciences). This tool has been chosen due to its popularity both in education and business sector. It provides different types of tests, their analysis and different forms of outputs. We use this tool specifically because The SPSS software package is frequently being updated and enhanced, so with each main revision comes a new version of that package. The package allows you to obtain statistics ranging from simple descriptive numbers to complex analyses of multivariate environments [35][36][37][38].

4.3. Data Analysis

Number of tests were run on the collected data to check the trends and the reliability of data. The tests are as follows:

4.3.1. Cross Tabulation and Cronbach's alpha

In social sciences, cross tabulation is used to find patterns, tendencies, and likelihoods in raw data [39][40]. The cross tabulation can be observed from the viewpoint of columns and rows. We checked the relationship of each variable with other in each question by the value of "Pearson Chi-Square" [41][42]. Pearson Chi-square test has been done to check the association between two variables. The value lies between 0.00 to 0.76 in our case for all variables. Cross tabulation results of the questions is shown below

Cronbach's Alpha is most commonly used reliability test in social sciences. It is referred as "internal consistency" reliability test [43][44][45]. We also applied this test to check the reliability of our data. All the results are greater than 0.50 which is good for any test. The Cronbach's Alpha value is also given below.

Table 1: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.957	.956	30

Internal consistency is shown by the value of the alpha coefficient for the five items. Value of alpha coefficient is 0.957, which is quite good.

Table 2: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.755	.771	3

Table 3: Cross Tab 1

1. Information Security Controls & Principles							
Knowledge							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	1	6	4	1	3	15
	Good	0	0	4	0	0	4
	Satisfactory	0	0	4	1	1	6
	Poor	0	0	1	1	0	2
	Very poor	0	0	1	5	0	6
	Total	1	6	14	8	4	33

Table 4: Cross Tab 2

1. Information Security Controls & Principles							
Practical							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	8	4	3	0	0	15
	Good	0	1	3	0	0	4
	Satisfactory	0	1	4	1	0	6
	Poor	0	0	1	0	1	2
	Very poor	0	0	3	3	0	6
	Total	8	6	14	4	1	33

Table 5: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.716	.700	3

Table 6: Cross Tab 3

2. Information Security Governance							
Knowledge							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	6	3	3	0	0	12
	Good	1	3	1	1	0	6
	Satisfactory	1	0	6	0	0	7
	Poor	0	0	0	2	1	3
	Very poor	0	0	0	4	1	5
	Total	8	6	10	7	2	33

Table 7: Cross Tab 4

2. Information Security Governance							
Practical							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	0	4	6	0	2	12
	Good	1	1	3	0	1	6
	Satisfactory	0	1	6	0	0	7
	Poor	0	0	1	2	0	3
	Very poor	0	0	2	3	0	5
	Total	1	6	18	5	3	33

Table 8: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.659	.701	3

Table 9: Cross Tab 5

3. Information Security Risk Management							
Knowledge							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	9	3	3	1	1	17
	Good	0	1	1	0	2	4
	Satisfactory	0	0	2	0	2	4
	Poor	0	0	1	1	0	2
	Very poor	0	0	4	2	0	6
	Total	9	6	12	5	1	33

Table 10: Cross Tab 6

3. Information Security Risk Management							
Practical							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	3	5	2	1	6	17
	Good	1	1	1	1	0	4
	Satisfactory	0	0	2	1	1	4
	Poor	0	0	1	1	0	2
	Very poor	0	0	4	1	1	6
	Total	4	6	10	5	8	33

Table 11: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.602	.603	3

Table 12: Cross Tab 7

4. Security and Audit Frameworks, Methodologies and Architecture							
Knowledge							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	1	2	6	1	3	13
	Good	0	3	2	1	0	6
	Satisfactory	0	0	2	2	0	4
	Poor	0	0	2	4	0	6
	Very poor	0	0	3	1	0	4
	Total	1	5	15	9	3	33

Table 13: Cross Tab 8

4. Security and Audit Frameworks, Methodologies and Architecture							
Practical							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	1	2	5	1	4	13
	Good	0	3	2	1	0	6
	Satisfactory	0	0	2	2	0	4
	Poor	0	0	2	4	0	6
	Very poor	0	0	3	1	0	4
	Total	1	5	15	9	3	33

Table 14: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.760	.756	3

Table 15: Cross Tab 9

5. Business Continuity Management							
Knowledge							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	7	3	0	0	0	10
	Good	1	1	2	0	0	4
	Satisfactory	0	1	5	0	0	6
	Poor	0	0	4	2	0	6
	Very poor	0	1	1	2	3	7
	Total	8	6	12	4	3	33

Table 16: Cross Tab 10

5. Business Continuity Management							
Practical							
Teachings		Excellent	Good	Satisfactory	Poor	Very poor	Total
	Excellent	1	3	2	3	1	10
	Good	0	1	1	0	2	4
	Satisfactory	0	0	5	1	2	8
	Poor	0	0	1	3	0	4
	Very poor	0	0	4	1	2	7
	Total	1	4	13	8	7	33

Table 17: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.601	.624	3

Table 18: Cross Tab 11

6. Access Management (Physical & Logical)							
Knowledge							
Teachings		Excellent	Good	Satisfactory	Poor	Very poor	Total
	Excellent	7	3	0	0	0	10
	Good	1	1	2	0	0	4
	Satisfactory	0	1	7	0	0	8
	Poor	0	0	2	2	0	4
	Very poor	0	1	1	2	3	7
	Total	8	6	12	4	3	33

Table 19: Cross Tab 12

6. Access Management (Physical & Logical)							
Practical							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	0	2	5	1	1	9
	Good	0	2	2	0	3	7
	Satisfactory	1	1	3	2	1	8
	Poor	0	0	2	0	1	3
	Very poor	0	0	2	3	1	6
	Total	1	5	14	6	7	33

Table 20: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.689	.699	3

Table 21: Cross Tab 13

7. Information Security Incident Management							
Knowledge							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	3	5	2	1	0	11
	Good	1	2	4	0	0	7
	Satisfactory	0	0	3	2	1	6
	Poor	0	0	2	1	2	5
	Very poor	0	1	0	3	0	4
	Total	4	8	11	7	3	33

Table 22: Cross Tab 14

7. Information Security Incident Management							
Practical							
Teachings		Excellent	Good	Satisfactory	Poor	Very poor	Total
	Excellent	3	5	1	2	3	11
	Good	2	3	1	1	2	7
	Satisfactory	0	1	2	3	0	6
	Poor	0	2	1	2	0	5
	Very poor	1	2	1	0	1	4
	Total	6	13	6	8	6	33

Table 23: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.722	.726	3

Table 24: Cross Tab 15

8. Operation Security Management							
Knowledge							
Teachings		Excellent	Good	Satisfactory	Poor	Very poor	Total
	Excellent	4	5	1	0	0	10
	Good	0	1	3	1	0	5
	Satisfactory	2	1	2	0	0	5
	Poor	0	1	3	4	0	8
	Very poor	0	0	0	4	1	5
	Total	6	8	9	9	1	33

Table 25: Cross Tab 16

8. Operation Security Management							
Practical							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	1	5	1	1	2	10
	Good	0	1	3	0	1	5
	Satisfactory	0	1	3	1	0	5
	Poor	0	1	3	3	1	8
	Very poor	0	0	3	1	1	5
	Total	1	8	13	6	5	33

Table 26: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.748	.764	3

Table 27: Cross Tab 17

9. Information Security Management System based on ISO27001							
Knowledge							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	2	9	2	1	0	14
	Good	0	0	1	1	0	2
	Satisfactory	0	0	6	1	1	8
	Poor	0	0	1	2	0	3
	Very poor	1	0	2	3	0	6
	Total	3	9	12	8	1	33

Table 28: Cross Tab 18

9. Information Security Management System based on ISO27001							
Practical							
Teachings		Excellent	Good	Satisfactory	Poor	Very poor	Total
	Excellent	2	6	3	2	1	14
	Good	0	0	1	1	0	2
	Satisfactory	0	0	4	3	1	8
	Poor	0	0	0	1	2	3
	Very poor	0	0	1	4	1	6
	Total	2	6	9	11	5	33

Table 29: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.780	.781	3

Table 30: Cross Tab 19

10. Understanding Organizational Behavior							
Knowledge							
Teachings		Excellent	Good	Satisfactory	Poor	Very poor	Total
	Excellent	5	3	2	0	0	10
	Good	1	3	4	0	1	9
	Satisfactory	0	0	4	1	0	5
	Poor	0	0	3	1	0	4
	Very poor	0	0	0	3	2	5
	Total	6	6	13	5	3	33

Table 31: Cross Tab 20

10. Understanding Organizational Behavior							
Practical							
		Excellent	Good	Satisfactory	Poor	Very poor	Total
Teachings	Excellent	1	5	1	2	1	10
	Good	0	4	3	1	1	9
	Satisfactory	0	0	3	1	1	5
	Poor	0	0	3	1	1	5
	Very poor	0	0	3	1	0	4
	Total	1	9	12	6	5	33

Table 32: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	40.726[a]	16	.001
Likelihood Ratio	34.725	16	.004
Linear-by-Linear Association	16.597	1	.000
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	28.738[a]	16	.026
Likelihood Ratio	30.365	16	.016
Linear-by-Linear Association	4.083	1	.043
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	40.726[a]	16	.001
Likelihood Ratio	34.725	16	.004
Linear-by-Linear Association	16.597	1	.000
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	28.738[a]	16	.026
Likelihood Ratio	30.365	16	.016
Linear-by-Linear Association	4.083	1	.043
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	43.980[a]	16	.000
Likelihood Ratio	45.503	16	.000
Linear-by-Linear Association	18.682	1	.000
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	27.472[a]	16	.037
Likelihood Ratio	27.055	16	.041
Linear-by-Linear Association	1.951	1	.162
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	43.980[a]	16	.000
Likelihood Ratio	45.503	16	.000
Linear-by-Linear Association	18.682	1	.000
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	29.181[a]	12	.004
Likelihood Ratio	31.203	12	.002
Linear-by-Linear Association	11.410	1	.001
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	16.787[a]	16	.399
Likelihood Ratio	20.800	16	.186
Linear-by-Linear Association	.703	1	.402
N of Valid Cases	33		

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20.515[a]	16	.198
Likelihood Ratio	21.650	16	.155
Linear-by-Linear Association	.658	1	.417
N of Valid Cases	33		

4.3.2. Frequencies

Survey Regarding Gap Analysis of Teachings and Practices in information security management (N=33)

The survey taken from 33 information security personnel within Islamabad from different organizations (one government and 15 non-government organizations) to analyze the gaps exists between teachings and practices of information security management. The purpose of this investigation is to find out the gaps in current course outline for information security

management being taught in SEECS NUST and implementations in IS industry and improve course outline accordingly. Following are the frequencies of each part of all 10 questions:

Table 33: Frequency Tests

1. Information Security Controls & Principles (Teachings)	**Frequency**	**Percent**
Excellent	15	45.5
Good	4	12.1
Satisfactory	6	18.2
Poor	2	6.1
Very poor	6	18.1
Total	***33***	100.0

1. Information Security Controls & Principles (Knowledge)	**Frequency**	**Percent**
Excellent	8	24.2
Good	6	18.2
Satisfactory	14	42.4
Poor	4	12.1
Very poor	1	3.0
Total	33	100.0

1. Information Security Controls & Principles (Practical)	Frequency	Percent
Excellent	1	3.0
Good	6	18.2
Satisfactory	14	42.4
Poor	8	24.2
Very poor	4	12.1
Total	33	100.0

2. Information Security Governance (Teachings)	Frequency	Percent
Excellent	12	36.4
Good	6	18.2
Satisfactory	7	21.2
Poor	3	9.1
Very poor	5	15.2
Total	33	100.0

2. Information Security Governance (Knowledge)	Frequency	Percent
Excellent	8	24.2
Good	6	18.2
Satisfactory	10	30.3
Poor	7	21.2
Very poor	2	6.1
Total	33	100.0

2. Information Security Governance (Practical)	Frequency	Percent
Excellent	1	3.0
Good	6	18.2
Satisfactory	18	54.5
Poor	5	15.2
Very poor	3	9.1
Total	33	100.0

3. Information Security Risk Management (Teachings)	Frequency	Percent
Excellent	17	51.5
Good	4	12.1
satisfactory	4	12.1
Poor	2	6.1
Very poor	6	18.2
Total	33	100.0

3. Information Security Risk Management (Knowledge)	Frequency	Percent
Excellent	9	27.3
Good	6	18.2
Satisfactory	13	39.4
Poor	5	15.2
Very poor	33	100.0
Total	9	27.3

3. Information Security Risk Management (Practical)	Frequency	Percent
Excellent	4	12.1
Good	6	18.2
Satisfactory	10	30.3
Poor	5	15.2
Very poor	8	24.2
Total	33	100.0

4. Security and Audit Frameworks, Methodologies and Architecture (Teachings)	Frequency	Percent
Excellent	13	39.4
Good	6	18.2
Satisfactory	4	12.1
Poor	6	18.2
Very poor	4	12.1
Total	33	100.0

4. Security and Audit Frameworks, Methodologies and Architecture (Knowledge)	Frequency	Percent
Excellent	5	15.2
Good	5	15.2
Satisfactory	14	42.4
Poor	7	21.2
Very poor	2	6.1
Total	33	100.0

4. Security and Audit Frameworks, Methodologies and Architecture (Practical)	Frequency	Percent
Excellent	1	3.0
Good	5	15.2
Satisfactory	15	45.5
Poor	9	27.3
Very poor	3	9.1
Total	33	100.0

5. Business Continuity Management (Teachings)	Frequency	Percent
Excellent	10	30.3
Good	4	12.1
Satisfactory	8	24.2
Poor	4	12.1
Very poor	7	21.2
Total	33	100.0

5. Business Continuity Management (Knowledge)	Frequency	Percent
Excellent	8	24.2
Good	6	18.2
Satisfactory	12	36.4
Poor	4	12.1
Very poor	3	9.1
Total	33	100.0

5. Business Continuity Management (Practical)	Frequency	Percent
Excellent	1	3.0
Good	4	12.1
Satisfactory	13	39.4
Poor	8	24.2
Very poor	7	21.2
Total	33	100.0

6. Access Management (Physical & Logical) (Teachings)	Frequency	Percent
Excellent	9	27.3
Good	7	21.2
Satisfactory	8	24.2
Poor	3	9.1
Very poor	6	18.2
Total	33	100.0

6. Access Management (Physical & Logical) (Knowledge)	Frequency	Percent
Excellent	3	9.1
Good	6	18.2
Satisfactory	13	39.4
Poor	6	18.2
Very poor	5	15.2
Total	33	100.0

6. Access Management (Physical & Logical) (Practical)	Frequency	Percent
Excellent	1	3.0
Good	5	15.2
Satisfactory	14	42.4
Poor	6	18.2
Very poor	7	21.2
Total	33	100.0

7. Information Security Incident Management (Teachings)	Frequency	Percent
Excellent	11	33.3
Good	7	21.2
Satisfactory	6	18.2
Poor	5	15.2
Very poor	4	12.1
Total	33	100.0

7. Information Security Incident Management (Knowledge)	Frequency	Percent
Excellent	4	12.1
Good	8	24.2
Satisfactory	11	33.3
Poor	7	21.2
Very poor	3	9.1
Total	33	100.0

7. Information Security Incident Management (Practical)	Frequency	Percent
Excellent	6	18.2
Good	13	39.4
Satisfactory	6	18.2
Poor	8	24.2
Very poor	33	100.0
Total	6	18.2

8. Operation Security Management (Teachings)	Frequency	Percent
Excellent	10	30.3
Good	5	15.2
Satisfactory	5	15.2
Poor	8	24.2
Very poor	5	15.2
Total	33	100.0

8. Operation Security Management (Knowledge)	Frequency	Percent
Excellent	6	18.2
Good	8	24.2
Satisfactory	9	27.3
Poor	9	27.3
Very poor	1	3.0
Total	33	100.0

8. Operation Security Management (Practical)	Frequency	Percent
Excellent	1	3.0
Good	8	24.2
Satisfactory	13	39.4
Poor	6	18.2
Very poor	5	15.2
Total	33	100.0

9. Information Security Management System based on ISO27001 (Teachings)	Frequency	Percent
Excellent	14	42.4
Good	2	6.1
Satisfactory	8	24.2
Poor	3	9.1
Very poor	6	18.2
Total	33	100.0

9. Information Security Management System based on ISO27001 (Knowledge)	Frequency	Percent
Excellent	3	9.1
Good	9	27.3
Satisfactory	12	36.4
Poor	8	24.2
Very poor	1	3.0
Total	33	100.0

9. Information Security Management System based on ISO27001 (Practical)	Frequency	Percent
Excellent	2	6.1
Good	6	18.2
Satisfactory	9	27.3
Poor	11	33.3
Very poor	5	15.2
Total	33	100.0

10. Understanding Organizational Behavior (Teachings)	Frequency	Percent
Excellent	10	30.3
Good	9	27.3
Satisfactory	5	15.2
Poor	4	12.1
Very poor	5	15.2
Total	33	100.0

10. Understanding Organizational Behavior (Knowledge)	**Frequency**	**Percent**
Excellent	6	18.2
Good	6	18.2
Satisfactory	13	39.4
Poor	5	15.2
Very poor	3	9.1
Total	33	100.0

10. Understanding Organizational Behavior (Practical)	**Frequency**	**Percent**
Excellent	1	3.0
Good	9	27.3
Satisfactory	12	36.4
Poor	6	18.2
Very poor	5	15.2
Total	33	100.0

4.3.3. Regression

It is the method to find out the relationship between two or more variables or if we want to predict the value of a variable based on the value of another variable. The variables that we want to predict are dependent variables and the variable that predicts the value is independent variable [46][47]. Our study model have four significant variables with values 0.25, 0.67, 0.47, 0.90 which means changes in these variables will cause significant effects in the study. The independent variable in our study is "does current course outline is sufficient for providing the required skills?" and the dependent variables are all the topics from course outline. The significant values of the four variables shows that these topics should must be improved to get the visible results. Table I shows the variables and their significance. The first column (model) indicates the initials of names of all the topics in course outline and second column shows their significance according to regression test.

Table 34: Regression Test

Regression	
Model	**Significance**
CP	**.025**
BCM	.294
AM	.273
SIM	.323
OSM	**.067**
ISO	**.047**
OB	.721
Interaction	.433
AMA	**.090**
SG	.577

4.3.4. Descriptive Statistics

Descriptive statistics shows range, mean, standard deviation and variances of all the responses [48][49]. The range of two variables were 3.00 and all other variables have the value 4.00.

Table 35: Descriptive Statistics

	N	Range	Maximum	Minimum	Mean	Std. Deviation	Variance	Skewness	Kurtosis			
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
T1	33	4.00	1.00	5.00	2.3939	.27157	1.56004	2.434	.657	.409	-1.091	.798
K1	33	4.00	1.00	5.00	2.5152	.19030	1.09320	1.195	.035	.409	-.639	.798
P1	33	4.00	1.00	5.00	3.2424	.17424	1.00095	1.002	.073	.409	-.282	.798
T2	33	4.00	1.00	5.00	2.4848	.25421	1.46033	2.133	.545	.409	-1.023	.798
K2	33	4.00	1.00	5.00	2.6667	.21614	1.24164	1.542	.062	.409	-1.012	.798
P2	33	4.00	1.00	5.00	3.0909	.15909	.91391	.835	.335	.409	.527	.798
T3	33	4.00	1.00	5.00	2.2727	.27618	1.58652	2.517	.820	.409	-.950	.798
K3	33	3.00	1.00	4.00	2.4242	.18479	1.06155	1.127	-.123	.409	-1.240	.798
P3	33	4.00	1.00	5.00	3.2121	.23338	1.34065	1.797	-.082	.409	-1.058	.798
T4	33	4.00	1.00	5.00	2.4545	.25780	1.48094	2.193	.494	.409	-1.258	.798
K4	33	4.00	1.00	5.00	2.8788	.19344	1.11124	1.235	-.184	.409	-.414	.798
P4	33	4.00	1.00	5.00	3.2424	.16301	.93643	.877	-.036	.409	.072	.798
T5	33	4.00	1.00	5.00	2.8182	.26634	1.53000	2.341	.158	.409	-1.394	.798
K5	33	4.00	1.00	5.00	2.6364	.21680	1.24545	1.551	.237	.409	-.702	.798
P5	33	4.00	1.00	5.00	3.4848	.18526	1.06423	1.133	-.124	.409	-.489	.798
T6	33	4.00	1.00	5.00	2.6970	.25183	1.44665	2.093	.371	.409	-1.119	.798
K6	33	4.00	1.00	5.00	3.1212	.20300	1.16613	1.360	.002	.409	-.528	.798
P6	33	4.00	1.00	5.00	3.3939	.18939	1.08799	1.184	.057	.409	-.628	.798
T7	33	4.00	1.00	5.00	2.5152	.24665	1.41689	2.008	.458	.409	-1.099	.798
K7	33	4.00	1.00	5.00	2.9091	.20115	1.15552	1.335	.058	.409	-.642	.798
P7	33	3.00	2.00	5.00	3.4848	.18526	1.06423	1.133	.208	.409	-1.173	.798
T8	33	4.00	1.00	5.00	2.7879	.26024	1.49494	2.235	.088	.409	-1.483	.798
K8	33	4.00	1.00	5.00	2.7273	.20072	1.15306	1.330	-.076	.409	-1.043	.798
P8	33	4.00	1.00	5.00	3.1818	.18695	1.07397	1.153	.260	.409	-.594	.798
T9	33	4.00	1.00	5.00	2.5455	.27210	1.56307	2.443	.407	.409	-1.335	.798
K9	33	4.00	1.00	5.00	2.8485	.17474	1.00378	1.008	-.073	.409	-.511	.798
P9	33	4.00	1.00	5.00	3.3333	.19784	1.13652	1.292	-.307	.409	-.612	.798

T10	33	4.00	1.00	5.00	2.5455	.25034	1.43812	2.068	.541	.409	-1.034	.798
K10	33	4.00	1.00	5.00	2.7879	.20761	1.19262	1.422	.084	.409	-.577	.798
P10	33	4.00	1.00	5.00	3.1515	.19030	1.09320	1.195	.293	.409	-.697	.798
Valid N (listwise)	33											

4.3.5. Open-ended Questions

Open-ended questions provide respondents freedom to share their views on a specific issue. For open-ended questions we adopted manual coding technique in which descriptive are defined according to the nature of questions being answered and then answers are being coded on these descriptive and percentage of responses is calculated [50][51]. The descriptive and responses against them shown in table 2 below.

Table 36: Open-Ended Coding

1.How do you think training in these topics can be improved?	
Descriptives	Responses
IS hands-on experience (by working on real case scenarios)	30 (90.9%)
IS lab sesions	3 (9%)
Neutral	0
2.At what level should graduates be trained in these topic?	
Basic Training compliance to organizational environment	16 (48.4%)
Expert-level Trainings	13 (39.3%)
Neutral	4 (12.1%)
3.What new topics, do you think should be added to the course outline?	
Study of NIST, ISACA and cobit standards, CISa CISM and GRC	4 (12.1%)
Reporting (Assessments report, Audit reports etc.), CEH, IT Audit	15 (45.4%)
Neutral	14 (42.4%)

Results and Findings

This chapter explains the final results we got after the analysis of all the questionnaires and responses from all information security personnel. This section summarizes the average results and views of practitioners on the gaps and how these gaps can bridge by taking small steps while designing curricula.

Information security practitioners better knows about the deficiencies and lack of ISM knowledge and skills in information security graduates because they have a direct dealing with graduates. As discussed, Pakistan is a developing country, so students rely specifically on knowledge provided in educational institutes and taking other courses and certifications are not economical for them. Almost six different kind of tests has been done in this study to show the gap between actual industry practices and teachings of ISM currently in Pakistan. Analysis was done on the current course outline of IS degree program of SEECS-NUST Islamabad.
By analyzing the responses and in the light of above performed tests, it was concluded that people working in information security industry thinks that graduates are not well-trained for industry. Although trend shows that topic selection in the current course outline of a SEECS-NUST is good enough, but the level of knowledge and skills students are getting are not enough for industry. Frequency results shows maximum responses that graduates have poor practical knowledge. They know the theory but most of them do not know how and when to use this knowledge. This needs to be improved.

5.1. Gap Analysis with Reference to Previous Studies

Previous studies also showed clearly the existence of a gap discussed above and also provided many ideas and approaches for designing and teaching ISM curriculum in educational institutes. In previous scholarly literature many reasons are given that are causing this gap and how instructors have more interest towards teaching technology oriented topics in information security rather security management related topics but literature present on this specific issue is very limited and this is an infant area in the research so more studies of this kind are needed to bridge this gap [1][3][4][11]. Many studies suggest that ISM can be taught in better way if instructors adopt teaching techniques that have more case studies in ISM curriculum [27][28]. Studies also provide evidences on how employee performance matters on the level of information security awareness they have [5][12]. Many researchers provide different techniques to enhance the security awareness level of employees in organizational environment. Although every organization have their own security policies that suits best for their organization but there should be a set of policies and rules that can be followed by all organizations

and ISM instructors should design their course outline compliance to these standards as analysis results showed that involvement of information security practitioners in ISM curriculum designing could prove to be beneficial.

5.2. Study Results: Likert Scale Questions Answered by Information Security Personnel

Table 37: Overall Average Results of Likert Scale Questions

Topics in course outline	Questions being asked		
	Do you think teaching this topic is essential and it does help prepare the students for the industry?	Do you think the knowledge and skills imparted from this topic meet your organization's standards?	Are the graduates equipped with skills and attitude for applying the knowledge in the practical field?
Information Security Controls & Principles	yes	yes	no
Information Security Governance	yes	no	no
Information Security Risk Management	yes	yes	yes
Security and Audit Frameworks, Methodologies and Architecture	yes	yes	no
Business Continuity Management	yes	yes	no
Access Management (Physical & Logical)	yes	no	no
Information Security Incident Management	yes	yes	no
Operation Security Management	yes	yes	no
Information Security Management System based on ISO27001	yes	no	no
Understanding Organizational Behaviour	yes	yes	no

The results shown in above table clearly indicates that all topics currently being taught are mandatory to provide necessary knowledge of information security management to students and the teaching style and standards and its outcomes also meet the

standard of their organizations somehow. Only few topics being taught needs to be improved but our targeted respondents showed us that students do not have enough skills and practical knowledge that are required to work in industry. Thus, hands on experience whether it is obtained from lab sessions in which students learn to work on risk management tools or any other tools that can be useful for information security professionals or conducting discussions and seminars in which students interact with information security personnel are necessary to bridge this gap that exists between ISM industry and academia in Pakistan.

5.3. Study Results: Open-Ended Questions Answered by Information Security Personnel

After Likert scale questions our questionnaire also had open-ended questions so that the respondents can get chance to suggest on how curricula designing and teaching can be improved as open-ended questions are the source to share detailed reviews and ideas about the topic. if we look beyond percentage and average results shown in the table 2 (chapter 4) we can undoubtedly claim that the factor that effects most and responsible for the existence of a gap is limited hands on experience provided to students in universities. Students are usually not familiar to ISM tools used by most of the IS practitioners. The best way to mitigate this limitation is to involve ISM industry practitioners in teaching ISM students by arranging seminars and discussion sessions with ISM practitioners in which students can get familiar with organizational environment.

Table 38: Average Results of Open-Ended Questions

Questions Being Asked	Average Answers
1.How do you think training in these topics can be improved?	IS hands-on experience (by working on real case scenarios)
2.At what level should graduates be trained in these topics?	Basic Training compliance to organizational environment
3.What new topics, do you think should be added to the course outline?	Reporting (Assessments report, Audit reports etc.), CEH, IT Audit

One of Open-ended questions response shows that 90% respondents agreed on teaching current topics in this course, can be improved by adding hands-on experience exercises with real organizational case studies, few lab sessions where students can learn about using ISM tools like tools for risk assessment, information security Metrix and other tools. In response to the question number 2 (open ended questions), 48% respondents said that Graduates should get basic trainings compliance to organizational environment. On answering last question 45% of respondents thinks that IT audit and audit assessment should be added as a separate topic in course outline of ISM as shown in Table 2 (chapter 4).

Conclusion and Future Work

This chapter presents concluding remarks about this study and limitations which leads to future work and can be helpful for future research.

6.1. Conclusion

This study presented the gap analysis of what is being taught in information security management and that being practiced in organizations of Islamabad, Pakistan. We identified this gap by conducting a survey from people working in organizations involve in performing information security management functions either by providing their services to other organizations as an external auditor or managing information assets within their own organization. Although most of these factors are not new and already present in scholarly literature available in security but their connection in curricula designing and industry practices have not been discussed clearly in literature. Additionally, few new factors that should be considered (IS lab session and seminars and session of students with IS practitioners) while teaching ISM are also discussed. information security practitioners have direct interaction with graduates so they can tell better that where the gap exists. Analysis of responses identifies the existence of gap and respondents also gave suggestions their suggestions on how teaching in ISM can be improved. information security management plays a vital role in securing organization's critical information assets so it is equally important for educational institutes to produce graduates that are equipped with skills to adjust in organizational environment and can use their skills as best as they can.

6.2. Future Work

As the limitation of this study, the point of view of students on what obstacles they face when they graduate and pursue information security management as career and what kind of improvements, they want in current curricula was not examined and this is the possibility for future research.

Moreover, this research has time constraints so, present study only examined the course outline of SEECS-NUST Islamabad, Pakistan and responses were taken from IS practitioners belonging to Islamabad, Pakistan only. Further extension of this study can be done by conducting survey in other cities of Pakistan and curricula of educational institutes offering information security degree program can also be evaluated on same pattern.

It would also be interesting to explore the shortcomings in the other courses being taught at the postgraduate level in Pakistan and also ISM curricula from other higher educational institutes.

This study can also be extended by making an online evaluation form which can take responses from information security personnel and information security researchers for information security instructors so they can evaluate and design information security management curriculum according to latest trends of industry.

Cybersecurity global index for 2018 shows that Pakistan listed into the list of countries with worst cybersecurity environment along with Bangladesh, Iran and Afghanistan [52]. This study can be compared with the state of all these countries because they have almost same cybersecurity index and same cybersecurity conditions, this will provide an international perspective to compare and improve the situation regarding gaps between ISM teachings and Practices.

References

[1] M. E. Whitman and H. J. Mattord, "Designing and teaching information security curriculum," p. 16, 2007.

[2] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing Employee Compliance with Information Security Policies : The Critical Role of Top Management and Organizational Culture," vol. 43, no. 4, pp. 615–659, 2012.

[3] M. A. Talib, A. Khelifi, and T. Ugurlu, "Using ISO 27001 in teaching information security," *IECON Proc. (Industrial Electron. Conf.*, pp. 3149–3153, 2012.

[4] A. Ahmad and S. Maynard, "Teaching information security management: Reflections and experiences," *Inf. Manag. Comput. Secur.*, vol. 22, no. 5, pp. 513–536, 2014.

[5] S. H. A. M, "Information Security Awareness within Business Environment: An IT Review," *SSRN Electron. Journa*, 2012.

[6] E. E. Tanner-smith and E. Tipton, "Robust variance estimation with dependent effect sizes : practical considerations including a software tutorial in Stata and SPSS," no. August 2013, 2014.

[7] "Pakistani banks hit by biggest cyber attack in country's history- Samaa Digital." [Online]. Available: https://www.samaa.tv/news/2018/11/pakistani-banks-hit-by-biggest-cyber-attack-in-countrys-history/. [Accessed: 24-Aug-2019].

[8] "Over 19,000 card details from 22 Pakistani banks stolen in cyber-securitay breach | Sci-Tech." [Online]. Available: www.geo.tv/latest/217471-cyber-attack-on-pakistani-banks-what-we-know-so-far.

[9] "Pakistan Ranked 7th Worst in Cyber-Security: Report." [Online]. Available: propakistani.pk/2019/02/14/pakistan-ranked-7th-worst-in-cyber-security-report/.

[10] "The state of cyber security - Newspaper - DAWN.COM." [Online]. Available: https://www.dawn.com/news/1445074. [Accessed: 24-Aug-2019].

[11] M. Mink and F. C. Freiling, "Is attack better than defense?," in *Proceeding InfoSecCD '06 Proceedings of the 3rd annual conference on Information security curriculum development*, 2007, p. 44.

[12] H. Rhee, Y. U. Ryu, and C. Kim, "Unrealistic optimism on information security management," *Comput. Secur.*, vol. 31, no. 2, pp. 221–232, 2011.

[13] "Why Every Company Needs an Information Security Program - Blog | KP." [Online]. Available: kirkpatrickprice.com/blog/why-every-company-needs-an-information-security-program/.

[14] D. L. Nazareth and J. Choi, "Information & Management A system dynamics model for information security management," *Inf. Manag.*, vol. 52, no. 1, pp. 123–134, 2015.

[15] E. Yeniman, G. Akalp, S. Aytac, and N. Bayram, "International Journal of Information Management Factors influencing information security management in small- and medium-sized enterprises : A case study from Turkey," *Int. J. Inf. Manage.*, vol. 31, no. 4, pp. 360–365, 2011.

[16] "'Cyber attacks -on banks expose online banking weaknesses' | Top Story | thenews.com.pk | Karachi." [Online]. Available: https://www.thenews.com.pk/print/389725-cyber-attacks-on-banks-expose-online-banking-weaknesses. [Accessed: 25-Sep-2019].

[17] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur.*, vol. 44, pp. 1–15, 2014.

[18] A. C. Yeo and L. Miri, "Understanding Factors Affecting Success of Information Security Risk Assessment : The Case of an Australian Higher Educational Institution," 2007.

[19] "Risk Management & Information Security Management Systems." [Online]. Available: www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms.

[20] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," *J. Inf. Secur. Appl.*, vol. 18, no. 1, pp. 45–52, 2013.

[21] "IT Risk Assessment - Pratum." [Online]. Available: www.pratum.com/services/it-risk-management/risk-assessment.

[22] D. Georg, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *J. Inf. Secur.*, vol. 4, no. 2, pp. 92–100, 2013.

[23] S. Harris, *All in One CISSP*. 2013.

[24] J. Järveläinen, "Information security and business continuity management in interorganizational IT relationships," *Inf. Manag. Comput. Secur.*, vol. 20, no. 5, pp. 332–349, 2012.

[25] R. A. Khther and M. Othman, "Cobit Framework as a Guideline of Effective it Governance in Higher Education: A Review," *Int. J. Inf. Technol. Converg. Serv.*, vol. 3, no. 1, pp. 21–29, 2013.

[26] L. Futcher, C. Schroder, and R. Von Solms, "Information security education in South Africa," *Inf. Manag. Comput. Secur.*, vol. 18, no. 5, pp. 366–374, 2010.

[27] M. Bishop, "Teaching context in information security," *J. Educ. Resour. Comput.*, vol. 6, no. 3, pp. 3-es, 2007.

[28] A. Nwala, "Teaching Information Security with Workflow Technology – A Case Study Approach," vol. 25, no. 3, 2014.

[29] W. Alec Cram and J. D'Arcy, "Teaching information security in business schools: Current practices and a proposed direction for the future," *Commun. Assoc. Inf. Syst.*, vol. 39, no. 1, pp. 32–51, 2016.

[30] M. Siponen, M. Adam Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, 2014.

[31] T. Sommestad and J. Hallberg, "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour," vol. 9, no. March, pp. 26–46, 2015.

[32] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "Information Security Management System Standards : A Comparative Study of the Big Five," no. October, 2011.

[33] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management

needs more holistic approach : A literature review," *Int. J. Inf. Manage.*, vol. 36, no. 2, pp. 215–225, 2016.

[34] R. Ullah, G. P. Shivakoti, and G. Ali, "Factors effecting farmers' risk attitude and risk perceptions: THE case of Khyber Pakhtunkhwa, Pakistan," *Int. J. Disaster Risk Reduct.*, vol. 13, pp. 151–157, 2015.

[35] D. Arkkelin, *Using SPSS to Understand Research and Data Analysis*. 2014.

[36] A. Ghasemi and S. Zahediasl, "Normality Tests for Statistical Analysis: A Guide for Non-Statisticians," vol. 10, no. 2, pp. 486–489, 2012.

[37] A. Spss and O. F. Analysis, "An SPSS R -Menu for Ordinal Factor Analysis," vol. 46, no. 4, 2012.

[38] "IBM SPSS Statistics 24 | SURFspot." .

[39] A. Butt, R. Shabbir, S. S. Ahmad, and N. Aziz, "Land use change mapping and analysis using Remote Sensing and GIS: A case study of Simly watershed, Islamabad, Pakistan," *Egypt. J. Remote Sens. Sp. Sci.*, vol. 18, no. 2, pp. 251–259, Dec. 2015.

[40] H. G. Cheng and M. R. Phillips, "Secondary analysis of existing data: opportunities and implementation," *Shanghai Arch. Psychiatry*, vol. 26, no. 6, pp. 371–375, 2014.

[41] M. J. Slakter, "A Comparison of the Pearson Chi-Square and Kolmogorov Goodness-of-Fit Tests with Respect to Validity," *J. Am. Stat. Assoc.*, vol. 60, no. 311, pp. 854–858, 1965.

[42] M. L. Mchugh, "Lessons in biostatistics The Chi-square test of independence," vol. 23, no. 2, pp. 143–150, 2013.

[43] M. Tavakol and R. Dennick, "Making sense of Cronbach's alpha," *Int. J. Med. Educ.*, vol. 2, pp. 53–55, 2011.

[44] D. G. Bonett and T. A. Wright, "Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning," *J. Organ. Behav.*, vol. 36, no. 1, pp. 3–15, Jan. 2015.

[45] K. S. Taber, "The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education," *Res. Sci. Educ.*, vol. 48, no. 6, pp. 1273–1296, 2018.

[46] N. Fumo and M. A. Rafe Biswas, "Regression analysis for prediction of residential energy consumption," *Renew. Sustain. Energy Rev.*, vol. 47, pp. 332–343, 2015.

[47] D. T. Bui, O. Lofman, I. Revhaug, and O. Dick, "Landslide susceptibility analysis in the Hoa Binh province of Vietnam using statistical index and logistic regression," *Nat. Hazards*, vol. 59, no. 3, pp. 1413–1444, 2011.

[48] A. G. Bedeian, "'More Than Meets the Eye': A Guide to Interpreting the Descriptive Statistics and Correlation Matrices Reported in Management Research," *Acad. Manag. Learn. Educ.*, vol. 13, no. 1, pp. 121–135, Mar. 2014.

[49] A. D. Ho and C. C. Yu, "Descriptive Statistics for Modern Test Score Distributions: Skewness, Kurtosis, Discreteness, and Ceiling Effects," *Educ. Psychol. Meas.*, vol. 75, no. 3, pp. 365–388, 2015.

[50] P. M. McQuirk and P. O'Neill, "Using questionnaires in qualitative research," *Qual. Res. Methods Hum. Geogr.*, pp. 246–273, 2016.

[51] "How to analyze open-ended responses | SurveyMonkey." [Online]. Available:

https://www.surveymonkey.com/curiosity/open-response-question-types/. [Accessed: 02-May-2019].

[52] "Securing Cyberspace for Pakistan." [Online]. Available: http://www.technologyreview.pk/securing-cyberspace-for-pakistan/. [Accessed: 29-Sep-2019].