SUPERVISOR CERTIFICATE

It is certified that the final copy of the MS thesis has been evaluated by me, found as per specified format and error free.

Dated: _____ _____

Thesis Supervisor
Brig. Dr. Ashraf Masood (Retd)

IMPLEMENTING INTERNATIONAL BEST PRACTICES IN ACADEMIC INSTITUTES

By

HUMA REHMAN

Submitted to the faculty of Information Security Department Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

August,2014

ABSTRACT

IMPLEMENTING INTERNATIONAL BEST PRACTICES IN ACADEMIC INSTITUTES

By

Huma Rehman

The academic institutions are among the most targeted information systems in the world. Their networking systems present a unique challenge in terms of information security. Their highly decentralized infrastructure makes it difficult to ensure reliable security measures across the networks. Moreover, academic institutes or universities have different departments, with diverse users (faculty, staff, students, and researchers), with abundant public and private data residing on servers and end systems, the probability and impact of threats and damage to the confidentiality, integrity and availability have never been higher. Although the educational institutes are now aware that the security of their information assets (including IT infrastructure, records, research data, faculty and students) is their highest priority in terms of risk, business continuity and reputation, however very little research/work has been carried out in this field. This research work provides a general framework for carrying out the risk assessment within the scope of ISMS and suggesting some best security measures in order to implement the Information Security Management System (ISMS) in academic institutes of Pakistan. The standard ISO 27001 of ISMS is selected to ensure the selection of appropriate security controls to protect information assets, however, other institutes are free to choose any other standard or method or combination of different controls or best practices according to their requirement.

To My Beloved Parents

ACKNOWLEDGMENTS

With deep sense of gratitude and appreciation, I am grateful to Almighty and Everlasting Allah, the most beneficial, merciful, all embracing, all knowing for His kindness to me in all spheres of life and who blessed me with the opportunity, courage and determination to accomplish this humble contribution towards knowledge.

My sincere and heartfelt thanks to my supervisor Brig (R) Dr.AshrafMasoud for the colossal support in my research, and for his patience and motivation. His guidance helped me in research and articulation of this thesis. I could not have imagined having a better advisor and mentor for my Masters study. Besides my advisor, I would like to thank the rest of my thesis committee: Lecturer Bashir Bilal, Lecturer AdeelaWaqar, and Lecturer Ayesha Naureen for their encouragement and insightful critique which helped me improve my work.

My special thanks to Mustafa Raza - IT Assurance and Services Professional, whose direction and assistance made it possible for me to accomplish this task.

Last but not the least, I would like to thank my parents and husband for supporting me spiritually throughout my academic career.

TABLE OF CONTENTS

List of Tables……………..…………………......…………………………………………….....i
List of Figures …….…......……………………………………………………………………....ii
List of Acronyms ..……………………………………………………………………….iii

1. INTRODUCTION 1
1.1 Overview 1
1.2 Background 1
1.2.1 Confidential or Sensitive Information: 2
1.2.2 Diverse Users and Access Methods: 2
1.2.3 High Risk Activities on Academic’s Network: 2
1.3 Information Security Threats Faced By Academic Institutes 3

2. LITERATURE REVIEW 5
2.1 Overview 5
2.2 Existing Methodologies for Information Security 5
2.2.1 ISP Methodologies: 5
2.2.2 Methodologies for Information Security Management System: 6
2.2.3 Risk Management: 6
2.3 Additional Contributions 7
2.4 ISMS Standards 8
2.4.1 BS 7799: 8
2.4.2 ISO 27001: 9
2.4.3 PCIDSS: 11
2.4.4 ITIL: 11
2.4.5 COBIT: 12
2.5 ISMS in Academic Institutions 12
2.6 Universities Following International Best Practices 15

3. IMPLEMENTING INTERNATIONAL BEST PRACTICES IN ACADEMIC INSTITUTES 17
3.1 Introduction 17
3.2 Implementation Methodology 17
3.2.1 Phase 1: 17
3.2.2 Phase 2: 20
3.2.3 Phase 3: 24
4. MIS CELL – A CASE STUDY 26
4.1 Overview 26
4.1.1 Existing Organizational Structure of MIS Cell: 28
4.2 Proposed ISMS Framework for MIS Cell 29
4.2.1 Phase 1: 29
4.2.2 Phase 2: 30
4.3 Risk Management – Examples 39
4.4 Formation of SOA 44
5. CONCLUSION 48
5.1 Introduction 48
5.2 Future Work 51
5.3 Conclusion 52
6. BIBLIOGRAPHY 53
7. APPENDIX A 56
8. APPENDIX B 64

LIST OF TABLES

Table Number **Page**

Table 3.1: Non-Applicable ISO 27001 Clauses for Academic Institutes 23

Table 4.1: Confidentiality Criteria 31

Table 4.2: Integrity Criteria 32

Table 4.3: Availability Criteria 32

Table 4.4: Asset Valuation Matrix (V) 32

Table 4.5: Threat, Vulnerability & Risks 33

Table 4.6: Probability of Risk (P) 37

Table 4.7: Impact of Risk (I) 37

Table 4.8: Risk Rating (R) 38

Table 4.9: Risk Assessment Sheet 43

Table 4.10: Statement of Applicability 47

LIST OF FIGURES

Figure Number **Page**

Figure 2.1: Plan-Do-Check-Act on BS7799 8

Figure 2.2: ISO 27002:2005 11

Figure 2.3: ITIL Components 12

Figure 3.1: Illustration of Information Risk Management Process 22

Figure 3.2: Graphic Representation of Proposed Framework 24

Figure 4.1: MIS Cell Internet Map 28

Figure 4.2: MIS Cell Organogram 29

Figure 4.3: MIS Cell Proposed Organogram 30

LIST OF ACRONYMS

BYOD	Bring-Your-Own-Device
CASE	Computer-Aided Software Evaluation
CIS	College Information System
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and related Technology
ERIMS	Equipment Repair and Inventory Management System
ISMS	Information Security Management System
ISM-TF	Information Security Management-Task Force
ISSA	Information Security System Auditor
ISO	Information Security Office
ISP	Information Security Plan
ITIL	Information Technology Infrastructure Library
LMS	Learning Management System
MIS	Management Information System
ORM	Online Registration Module
P2P	Peer-to-Peer

PCDISS	Payment Card Data Industry Security Standard
RIMS	Resource Information and Management System
RMS	Result Management System
SAMS	Student Attendance Management System
SOA	Statement of Applicability

Chapter 1

1. INTRODUCTION

1.1 Overview

Information Technology infrastructures have indubitably been prone to threats and been at risk, due to varied intentional / unintentional user-end errors or malevolent actions, since the inception. The interconnectivity of computer systems, though offers convenience of life to the masses, it also enhances susceptibility of the system to these threats. In addition, individuals with advanced IT skills ensuing network intrusions, data theft, hacking etc. is increasing through internet and other media.

1.2 Background

Before the advent of computers, the paper records were maintained and safeguarded by the administrators of educational institutes in filing cabinets. The cabinets were locked and the offices were also locked as a further precaution. In recent years, however, the education institutes have joined other entities to adopt technology as primary means to organize and access information.Sharing information via computers and networks has proven to be an economical way of getting things done. Thus, they rely more on computers now and this is likely to increase.

The Educational institutes in Pakistan face a barrage of information security incidents such as data theft, malicious software infections, hacking and intrusion through networks due to lack of trained or qualified IT staff. Adversarial effects of these incidents include compromised private and intellectual properties / data, considerable financial losses, and potential threats to critical IT infrastructure. In spite of these issues, little research has been conducted at this level.

These institutes are vulnerable to exploitation due to several reasons which include:

1) Diverse user community (students, faculty and staff etc.).
2) Abundant private and research information.

a) Time critical operations (like start and end of semesters, exam schedules, result announcement etc.).

b) Variety of data that is piling up every passing day (e.g. student registrations, accounts, exams, degrees/diplomas, awards, results etc.).

3) Open networks with significant bandwidth, high end-user turnover and at-risk activities.

4) Decentralized IT system.

5) Extensive cyber links with government, military, private sector, and other academic institutions.

6) Permission to Bring-Your-Own-Device (BYOD) to instructors and students.

1.2.1 Confidential or Sensitive Information:

Academic institutions have personal information of faculty, staff, students, alumni, and researchers (e.g., CNICs, date of birth, financial and medical information, grades, telephone numbers, and permanent addresses). Furthermore, these institutes conduct research and development for all technology innovations in the country. However, some institutes may secure this private data and intellectual property through strict IT security policies; but there is still a huge gap that endangers the security of personal and intellectual information.

1.2.2 DiverseUsers and Access Methods:

The academic networks are normally used by different users with different responsibilities and access methods. Users include students, faculty, staff, contractors, and guests. They access institutions' systems through on-campus and remote logins from different locations (e.g. conference halls, classrooms, computer labs and other campuses).

1.2.3 High Risk Activities on Academic's Network:

Academic network users are in habit of using internet openly on their personal laptops, PDAs, smart phones for different purpose. This gives rise to performing high risk

activities on the network like peer-to-peer sharing (P2P), instant messaging, downloading and e-learning. Thus, making academic institutions at high risk due to their networks' open culture.

1.3 Information Security Threats Faced By Academic Institutes

Academic institutes face information security threats from insiders (e.g. students, faculty etc.) as well as from outsiders (e.g. hackers, script kiddies etc.). These threats have raised serious concerns for academic networks as most of the attacks may go unnoticed or undetected (stealth attacks) due to lack of proper controls and countermeasures to evade these risks. Moreover, time critical activities offer very less time to detect and identify security incidents. It should also be noted that for academic institutes the integrity of information is more important than its confidentiality. For instance, Higher Education Commission requires to verify the record of a student who left the institute 20 years ago. Confidentiality is not required in that case but integrity of that record holds more value in terms of C, I, A.

Moreover, academic network administrators have difficulty to manage thousands of nodes. Thus, covert attacks or other security breaches are only identified by coincidence.

Attackers use different exploitation techniques to gain access to the information systems. New software vulnerabilities are exploited on daily basis but five of these vulnerabilities are top priority for educational institutes:

1) MySQL Injection
2) Sun Java Buffer Overflow
3) Adobe Acrobat SING Buffer Overflow
4) Mail Server Misconfiguration
5) VNC Authentication Bypass.

In spite of critical information security threats faced by academic institutions, very little research has been conducted on the need of implementing information security management system and designing policies to cope with these security threats.

Implementing international best security practices is not one time process but it is a continuous process. Its first step is to define the scope and then to continuously assess the risk associated with the information assets. Risk assessment is the basic element of risk management.

Therefore, an existing international ISMS standard ISO/IEC: 27001 is followed to assess the risk. This thesis will take MIS Cell of Military College of Signals – NUST as a case study. Asset based risk assessment approach is defined and performed against the critical assets of MIS Cell. The risk assessment procedure generally include the following steps:

1) Asset valuation
2) Identifying threats
3) Identifying vulnerabilities associated with threats identified in step 2
4) Estimating the impact of these vulnerabilities on business operations
5) Estimating the likelihood of occurrence of these vulnerabilities
6) Calculating risk value (quantitative or qualitative)
7) Suggesting controls or countermeasures to reduce/avoid or mitigate risk

So after performing the risk assessment, the Statement of applicability (SOA) of ISO 27001 controls is designed. Based on this SOA, administration will decide whether to implement that control or accept the risk as it is. Threat to information security can never be eliminated completely but one can provide defence in depth to avoid security breaches. Thus, in the end some generic controls, which every academic institute must implement, are suggested to minimize the risk of information security breaches.

Chapter 2

2. LITERATURE REVIEW

2.1 Overview

Information is a vital and fundamental asset in today's Information Technology (IT) – enabled world. In order to support decision-making processes access to high-quality, comprehensive, accurate and up-to-date information is needed. Thus, to ensure that resources are well protected, it is extremely important to secure information system resources. Information security is not just a simple matter of usernames or passwords [1].With the increasing number of viruses, worms, Trojans, hackers, phishers and social engineers day by day, it is almost impossible to remain secure on the internet. So it is necessary for an organization to use an Information Security Management System (ISMS) to efficiently manage their IT assets.

2.2 Existing Methodologies for Information Security

Security refers to "*minimizing the risk of exposure of assets and resources to vulnerabilities and threats of various kinds*". The three basic qualities of information security: Confidentiality (C), Integrity (I) and Availability (A) need to be protected at all times. Thus, the existing methodologies related to information security issues can be categorized into three groups i.e.:

2.2.1 ISP Methodologies:

These methodologies do not provide security controls and risk concept rather they provide the method to create information security plans. Examples are *METHOD/1* (which simplifies the process of developing systems by breaking down each phase into 'segments'), *IE Expert* (provides planning, re-engineering and developing integrated information systems) [2], *VIP-2000*(consists of four levels: Patterns and Scenarios, Road map, Components (ISPM, EIII, EJMS, S3IE, UMT), repository) [3].

2.2.2 Methodologies for Information Security Management System:

These methodologiesmainly focus on policy designs. However, lack in provision of integrated architecture, analysis and modelling tools. For instance, *NIST handbook* (helps in securing computer-based information by explaining important concepts, cost consideration, techniques and approaches for security controls) [4].

2.2.3 Risk Management:

It focuses on asset-based analysis approach. No concern on alignment of security strategy with other strategies and has no concept of security controls. These methodologies are further divided into two groups:

1) Quantitative Risk Analysis

It is based on loss exposure as a function of the vulnerability of an asset to a threat multiplied by the probability of threat becoming a reality. It includes ALE (Annualized Loss Expectancy) [5], Courtney Method [6], Stochastic Dominance [7]. Quantitative risk analysis methodologies have some disadvantages. E.g. estimating the loss of each IT asset is imprecise. Also the probability of distribution of losses is highly skewed. There are certain situations which cause minor problems, some can cause major problems but this approach tends to average these events, thus, smudging the differences between the extreme situations and implying similar solutions. They cannot define the contingency plan an organization should use.

2) Qualitative Risk Analysis

It is based on assumptions (or descriptive variables) that certain amount of threat cannot be expressed in discrete quantity or number and precise information cannot be obtained. It includes scenario analysis method [8], fuzzy matrices approach [9], Delphi techniques, Questionnaires [10]. Delphi technique can be used with any of these methodologies and it is useful when the participants are not in physical proximity. However, qualitative risk

analysis methodologies are inaccurate. The variables (e.g. High, Medium, and Low) must be clearly explained to all entities involved in risk analysis.

2.3 Additional Contributions

Sangkyun Kim and ChoonSeongLeem[11] proposed a framework for security of information systems which emphasizes on the planning of information security controls, provide the steps and tools for planning and aligns the security strategy with other strategies. However, in order to make this strategy work, a lower-level process model is needed to be developed to provide step by step guidance to the organization. Also it requires the development of evaluation model for security controls.

Another methodology is proposed by Mengquan Lin, Qiangmin Wang, and Jianhua Li [12] for quantitative risk assessment for information security. In the proposed method, the four attributes of information security i.e. confidentiality, integrity, availability and controllability are evaluated separately. After constructing the risk model based on above attributes, they assign weights for the criteria. They develop a method for constructing weight. The method is called MMCW (Mixed Method of constructing weights), which is based on Delphi Method and Analytical Hierarchy Process (AHP).

Another work of ChoonSeongLeem, Sangkyun Kim and Hong Joo Lee [13] proposed an evaluation methodology for ISMS which consists of evaluation indices, evaluation process, and maturity model. Evaluation indices consist of four domains i.e. plan level, environmental level, support level, technology level. Maturity model has five maturity levels i.e. Strategic (i.e. ISMS create new business opportunities), Management-active (i.e. best practices of ISMS are reviewed periodically), Management-passive (i.e. information security strategic planning is established), Technical (i.e. technical controls of premises security are established) and Functional (i.e. security controls like anti-virus, password protection, etc are functional). Evaluation process consists of preparation (e.g. project initiation, resource planning), assessment (qualitative or quantitative, data gathering), analysis (analysis of assessment results and report generation) and

management (feedback, reviews etc.). Based on above methodology the current and on-going status of ISMS can be analyzed or evaluated.

2.4 ISMS Standards

ISMS is basically a management framework for identifying important information, continuously evaluating security risks to identified information and taking reasonable steps on it. Since Information security plays a vital role in performing or executing the activities of an organization, a standard is needed to regulate governance over information security [14]. There are many IT governance standards that lead to information security but following five standards are widely used by the organizations for ISMS. These are BS 7799, ISO 27001, PCIDSS, ITIL and COBIT.

2.4.1 BS 7799:

BS 7799 is a British standard published in1995. It consists of several parts. The first part contains the best practices for ISMS which was later adopted by ISO as ISO 17799 "*information technology – code practice for information security management"*. The second part BS 7799-2 "*information security management system – specification with guidance for use"* focused on how to implement ISMS which later became ISO 27001 in Nov 2005 [15]. It introduces the Plan-Do-Check-Act model.

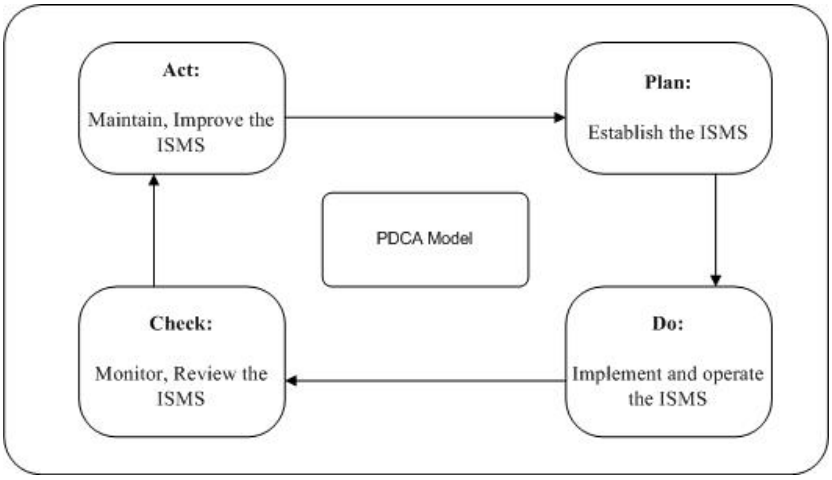


Figure 2.1: Plan-Do-Check-Act on BS7799

In PLAN phase, scope of ISMS is defined. Assets that need to be protected are identified, then risk assessment is carried out. In Do phase, risk treatment plan and controls are implemented. In CHECK phase, the effectiveness of risk treatment plan is reviewed and evaluated and in ACT phase, necessary corrective measures are taken to improve the process.

2.4.2 ISO 27001:

ISO 27001 specifies the need for establishing, implementing, operating, monitoring, reviewing, maintaining, improving a documented ISMS in an organization [14]. It is designed in such a way to ensure the selection of appropriate security controls in order to protect the information assets [15]. It also follows a PDCA model, in order to establish, implement, monitor, and improve the effectiveness of ISMS [16]. There are well defined steps in each phase [20].

1) PLAN PHASE

It consists of following steps:

a) Define Scope of ISMS
b) Define ISMS policy
c) Define Risk assessment approach of the organization
d) Identify the Assets
e) Identify the Risks
f) Analyze risk treatment option
g) Selecting controls for the treatment of risks
h) Obtaining management approval for and authorization for risk treatment
i) Preparing “statement of applicability”

2) DO PHASE

It consists of the following steps:

a) Define and implement risk treatment plan

b) Selecting suitable controls

c) Define how to measure the effectiveness of controls

d) Implement training and awareness programs

e) Implement security incident and response procedures

3) CHECK PHASE

Check phase comprises of the following steps:

a) Execute monitoring and review procedures

b) Measure the effectiveness of controls

c) Review risk assessment and review residual risk

d) Conducting internal audits

e) Updating security plans, if necessary

4) ACT PHASE

In this phase, following steps are taken:

1) Implement the identified improvements in ISMS

2) Take appropriate corrective and preventive measures

3) Ensure that improvements achieve their intended objectives

The subset document ISO 27002 has 133 distinct security controls under these 11 areas: Security policy, organizing information security, asset management, human resources security, physical and environmental security, communication and operation management, access control, information security acquisition development and maintenance, information security incident management, business continuity management, and compliance.

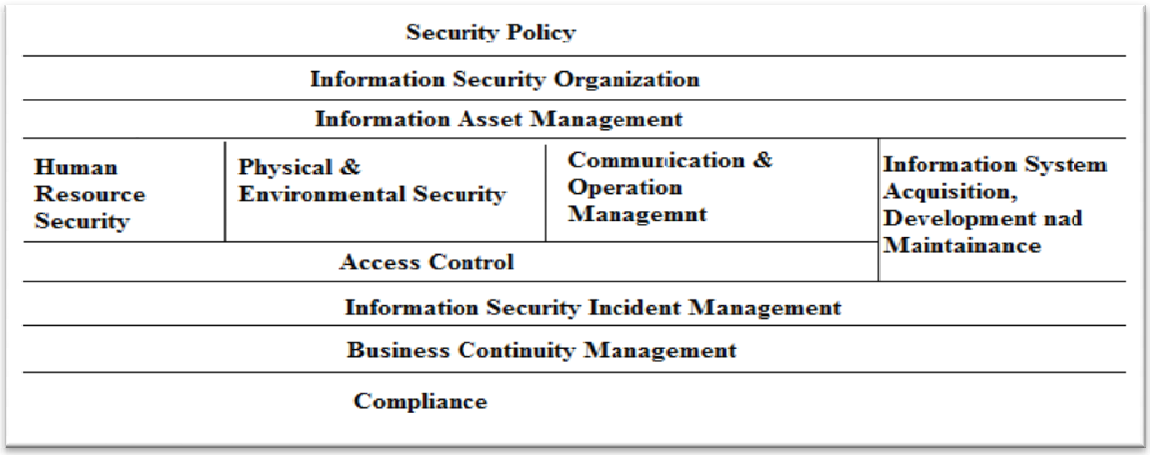


Figure 2.2: ISO 27002:2005

It can be adopted by any kind of organization – private or public.

2.4.3 PCIDSS:

The Payment Card Industry Data Security Standard (PCDISS) was created to help the organizations that process card payments to prevent credit card fraud with the help of increased controls around data and its exposure to compromise [17]

2.4.4 ITIL:

Information Technology Infrastructure Library (ITIL) is actually a set of concepts and practices for Information Technology Services Management (ITSM). It is originated as a collection of books containing 8 main components i.e. Security Management, Software Asset, Service Support, ICT Infrastructure Management, Service Delivery, Application Management, Small-Scale Implementation and Planning to Implement Service Management [18].

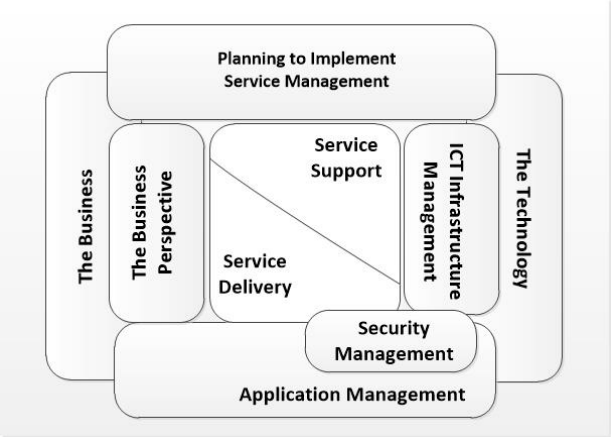


Figure 2.3: ITIL Components

2.4.5 COBIT:

Control Objectives for Information and related Technology (COBIT) was created by ISACA in 1996. It is an IT governance framework and supporting tools set that allows managers to bridge the gap between control requirements, technical issues, business risks, and security issues [14]. It has five IT governance areas: Strategic alignment, Value delivery, Resource management, Risk management, and performance measure [19].

2.5 ISMS in Academic Institutions

Information security has become a major issue for IT-related organizations especially those who rely on internet as a delivery medium. This fact is well realized by the industry e.g. the banks but it is not well realized by the academic institutions. Academic institutes rely on digital information to carry out various academic as well as administrative functions. They face unique information security threats and incidents like data theft, malicious software infections, hacking computers, infiltration of other entities via their networks, website defacement, unauthorized usage of internet bandwidth etc. The academic institutions are vulnerable to these threats due to several reasons [21]:

1) Abundant private and research data
2) Relatively open networks with significant bandwidth
3) High end user turn-over

4) Decentralized structure

5) Extensive cyber links with government, private or other educational institutions

6) Diverse range of users

The academic institutes have sensitive information. They have the private information of faculty, staff, students, alumni and researchers. The private information include NIC no., date of birth, academic qualifications, grades, personnel phone numbers, home addresses, email IDs etc. Moreover, they conduct research and development projects with the collaboration of industry as well. Each data type requires different security service. For instance, registration data needs integrity and availability, exam data needs confidentiality and protection against DOS attacks, thus, making availability of that data on time to the user. Similarly, financial records needs accuracy, thus, maintaining the integrity. In short, this private and intellectual property needs to be protected.

Academic institutions have diverse range of users. They have researchers, students, faculty, clerical staff, and IT-related personnel with each having different roles and responsibilities. They access the institute's system or network through different means e.g. via remote login, guest/personnel user account, VPN etc. The information security threats may originate from inside (e.g. students, faculty) as well as from outside (e.g. guest user). Any intruder who has malevolent aim can exploit the vulnerabilities with a little risk of getting caught.

Educational institutes provide excellent targets and may provide opportunity to sensitive targets with which they share information. The Skatta incident, in which several research institutes, military bodies and NASA were breached by Swedish teenager student (CNN.com, May 10, 2005), explains the vulnerabilities of these institutes. Terrorist may exploit these vulnerabilities and cause harm [21]. These attacks can be active or passive. Thus, leading to data theft, financial loss, reputation loss of that institute.

Regardless of these important information security issues faced by the academic institutes, little research is done in managing the information security of institutes. SteffaniA.burd, focused on the objective data and develops a practical roadmap for policy

and framework. He designed three methods: i) quantitative field survey, ii) qualitative one-to-one interview, and iii) empirical assessment of institute's network activity [21]. He concluded that academic institutions are creating a baseline level of security. He developed a roadmap for recommended policy and practices based on risk management approach.

Dana DesPlanques[22] suggested an information security policy framework for higher education. She divided it into two phases. At first phase, she suggested to review the existing policies of the university and make risk assessment. At second phase, based on phase 1 findings, a comprehensive information security policy, procedures and guidelines were developed to prevent security breaches.

D.S. Bhilar, A.K. Ramani and Sanjay Tanwani[23] proposed an information assessment plan for small, medium and large academic institutes. He proposed a Role-Based Direct Reporting System and develop a mechanism for the assessment of security metrics for institute's policies. According to him, for a particular metric when a threshold value is violated, it is detected by online network monitoring software. This will activate a search in database system for a point of contact (personnel) for that particular exception. After getting required information, SMS or e-mail is sent to that personnel and remedial action is planned and implemented.

Some of the security breaches reported in newspapers in previous 5 years are discussed below. Only the security breaches occurred in educational institutions from all over the world are discussed here:

1) On December 21, 2009 HIPPA security and privacy [24] published that over 600 patients at the University of California, San Francisco are being notified of a possible data breach that occurred when a hacker obtained e-mails containing their personal information. **Problem:** Hacking
2) On May 23, 2013 the Information security officer of University of Nebraska, USA, found that a critical database *Nebraska Student Information System (NeSIS)*

from university school system had been compromised. The NeSIS had the personal details of 654,000 students. **Problem:** Passwords hacked and revealed.

3) In University of Colorado, a server (which contained 44,998 student names and their social security number) was infected because it has vulnerable application running which was not properly patched. **Problem:** Missing patches and updates [25].
4) On May 8, 2006 four hard drives sold on eBay that has thousands of classified documents, confidential memos to the CEO, and employee names and SSNs[26]. **Problem:** Insecure disposal and re-use.
5) On July 17, 2011, NUST entry Test paper was leaked. **Problem:** Disgruntled employee, insufficient security measures [27].
6) In February 2010, a university in Georgia experienced a data breach of an internal server of the university where attackers were able to penetrate into the system and gained access to approximately 170,000 records from a university database [28].

2.6 Universities Following International Best Practices

One cannot implement ISMS or achieve the status of ISO 27001 at once, it demands apt considerations and requires time. There is a need to set the baseline first. Many academic institutes have started to take information security seriously. For instance, *University of Virginia-USA* has its own Risk Management department and they are analysing the risks for their assets regularly. Risk assessment is the first step for implementing ISMS. It should be kept in mind that in order to provide an organization the depth of information security management system's documentation, three options for ISMS development are available. Basic, Standard and Advanced. Organization selects the level according to its need and budget. The three levels are intended to provide different ISMS development frameworks. [29]

Basic: To establish the framework for ISMS, security policy and all required high level policies for the organization are implemented at this level.

Standard: At standard level, organization develops general purpose standards and policies needed to implement ISMS. Thus, all requirements for ISO27001 compliance are completely satisfied at this level.

Advanced: In order to establish complete ISMS at an advance level, organization develops all required policies, technical & general purpose standards, procedures and guidelines.

Hence, institute or an organization starts from basic level and reached the advance level within defined timeline.

Educational institutes that are accredited by ISO 27001 certification are: European Academy, Bozen – Italy, Warnborough College, UK, Free University of Bozen-Italy, Georgia State University-USA, King Abdul-Aziz University-KSA. They identified risks, threats, and created preventive and corrective action plans according to ISO publications. A few universities like University of Manchester-UK [31] have made only university IT security policies from ISO 27001 and BS 7799 standards.

Keeping in view the above discussion, it is important to implement best practices in the academic institutions of Pakistan as well to keep our institutions secure from cyber-attacks. For this purpose, first of all there is a need to design the framework for implementing these practices, what are the phases, how risk assessment should be done and what practices should all Pakistani institutes at least follow. So if, an institute starts from the basic level, it can gradually achieve the standard level.

Chapter 3

3. IMPLEMENTING INTERNATIONAL BEST PRACTICES IN ACADEMIC INSTITUTES

3.1 Introduction

Security of IT systems has never been given due consideration until recently. The main problem is two way: Firstly, the administration had not previously solicited the recommendations and requirements of experts from IT institutes. Secondly, IT staff of non-IT institutes lack the technical security related expertise. In former case, IT people are busy with their core responsibilities and do not have time to spend investigating and regularly maintaining IT security systems. In later case, IT people are not properly evaluated during hiring process and/or competitive salaries are not offered to right people. In this chapter, a framework for implementing ISMS in academic institutes of Pakistan is proposed.

3.2 Implementation Methodology

Leaving the huge task for securing institute's information systems to just one group (i.e. centrally administrative IT security department) is inappropriate. The reason is, it will be practically impossible to enforce any policies or to verify that policies are being followed in true sense by others. So everyone has to take part in this mission and has to realize his sense of duty. The proposed methodology is divided into three phases.

3.2.1 Phase 1:

In first phase, institutes must hire information security professionals. They have the responsibility to develop and implement information security matters. Phase 1 require full management commitment. New posts are suggested which are important because for effective and efficient handling of exceptions (in terms of information security), the

normal hierarchical system of academic institute is not enough. In information security management the time taken to respond on particular incident is very crucial. The suggested posts and their key responsibilities in terms of information security are as follows:

1) Information Security Management Task Force (ISM-TF)

The ISM-TF team should have the representatives from academic administration, HR, IT and senior management. They will co-ordinate to implement the ISMS, security measures and policies. This team will approve the methodologies and processes for ISMS.

2) Chief Information Security Officer (CISO)

The key responsibilities of CISO include:

a) Provides strategic and tactical planning, development, evaluation, and coordination of the information and technology systems for the network.
b) Facilitates communication between staff, management, vendors, and other technology resources within the institute.
c) Oversees the back office computer operations of the affiliate management information system, including local area networks and wide-area networks.
d) Designs, implements, and evaluates the systems that support end users in the productive use of computer hardware and software.
e) Develops and implements user-training programs on universities' information security policies and best practices.
f) Develop and present information security policies, procedures and guidelines for institute and get it approve from top management.
g) Supervise the ISMS implementation.

3) Information Security Officer (ISO)

The responsibilities of ISO include:

a) Monitoring to detect the security breaches related to institutes' information security policies
b) Manages the information security incident response
c) Developing the related security solutions

4) Internal Auditor

The main responsibilities of internal auditor include:

a) Evaluating the risk management of the institute and develop a report that describes that controls and measures are functioning as intended and helps to meet institutes' information security goals and objectives.
b) Reporting issues related to risk management and internal controls deficiencies.
c) Performing internal audits frequently and presenting audit reports to CISO.
d) Evaluating in terms of institute's information security, regulatory compliance program and disaster recovery.

However if the institute is small and doesn't have enough resources, it may divide the above mentioned responsibilities to their existing employees but proper information security awareness is mandatory for this purpose. For instance, the responsibilities for a network administrator and system administrator (besides regular responsibilities) in terms of information security will then include:

5) Network Administrator

Besides the responsibilities of dealing with physical network, including network devices i.e. switches, routers etc. following security responsibilities shall also be included in its role:

a) Applying relevant security patches
b) Hardening the network
c) Managing administrative credentials of network devices
d) Preparing procedures in order to implement the information security policies in local environment

6) System Administrator

Besides the regular responsibilities of system administrator, following responsibilities shall also be included in the job description of system administrator:

a) Hardening the end points (laptops and desktops) and servers.
b) Conducting security scans on all end systems, applying relevant patches and updating.
c) Installing, configuring and monitoring the anti-malware tools as per institute's security policies and procedures.
d) Taking regular back up of critical assets.
e) Reviewing and monitoring the user accounts and application privileges on network devices.

The advantage of above proposed structure will help to identify the non-performing roles in the institute and they will be accountable for any information security violations. Moreover, it will be helpful in smooth communications to the concerned personnel in right time, reducing the overall time for reaction in case of incident.

Moreover, determine the scope of ISMS and then define the security policy. The scope determines what information assets are exactly needed to be protected.

3.2.2 Phase 2:

After completing the objectives of phase 1 (i.e. hiring of professionals and training the staff for ISMS, defining the scope of ISMS), phase 2 will be commenced. In the beginning of phase 2, CISO along with his team of ISOs design an information security policy and regulations documents. All UK universities are members of the Universities and Colleges Information Security Association (UCISA), which has produced a template and guidance document so that each of their members can make their policies according to their own environment [31]. The same set of guidelines can be modified and used as a basis for the production of information security policies and regulations for Pakistani institutes. The document guides on making policies for information handling, user management,

acceptable use of computers, system management, network management, software management, business continuity planning, compliance.

Moreover, in phase 2, perform the risk management which is the building block for implementing ISMS. Various procedures, tools and methodologies have been developedfor risk management before. However, in the proposed solution for the implementation of ISMS, ISO 27005 [32] risk management standard is proposed for ISMS risk management. According to this standard, the risk management framework consists of these steps: **Context establishment** (requires all the organization information that will assist to define the basic criteria, scope and boundaries, and organization for Information security risk management), **risk assessment** (contains risk identification, risk analysis, and risk valuation), **risk treatment**, **risk acceptance**, **risk communication and consultation, risk monitoring and review**[1]. The process of this standard is mapped on ISO 27001 in such a way that:

1) In ISO/IEC 27001:2005, the term "context" is not used. However, all of Clause 7relates to the requirements "define the scope and boundaries of the ISMS" [4.2.1 a)], "define an ISMS policy" [4.2.1 b)] and "define the risk assessment approach" [4.2.1 c)], specified in ISO/IEC 27001:2005.

2) ISO/IEC 27001:2005 [Clause 5.2.1] concerns establishing the resources for the implementation and operation of ISMS.

3) Risk acceptance criteria of ISO 27005 resemble to "criteria for accepting risks and identify the acceptable level of risk" specified in ISO/IEC 27001:2005 [Clause 4.2.1 c) 2)]

Following diagram shows the process of risk management in ISO 27005:

[1] It is noted that risk communication and consultation, and risk monitoring and review are not part of the thesis

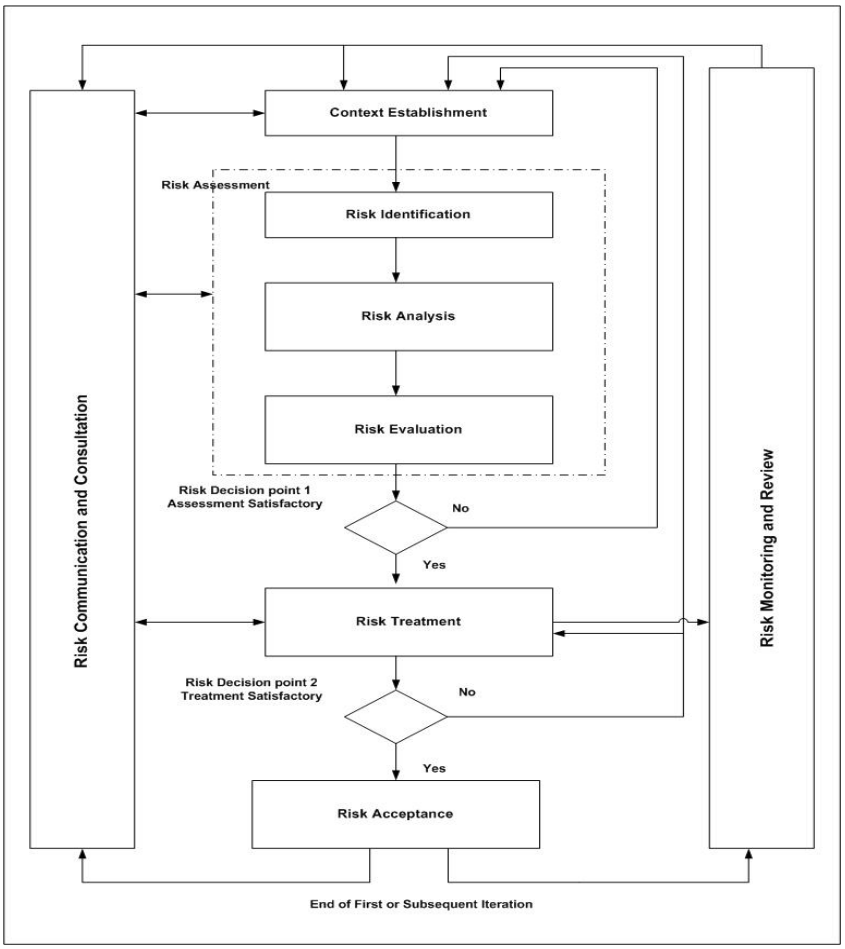


Figure 3.1: Illustration of Information Risk Management Process

During risk management, first step is the identification and classification of assets. Asset is anything that has value to the institute. It can be documents, hardware, software and people. So asset identification is making a list of important assets of the institute according to the ISMS scope. Whereas, asset classification involves categorizing the assets in terms of confidentiality, integrity and availability.

The next step is the risk analysis. In this step, risks are identified against each asset and classified according to their severity and vulnerability. These risks are evaluated and assigned values (either quantitative or qualitative).

Then finally risk treatment is performed. Risk treatment is the process of applying suitable controls to reduce the level of identified risks. These controls can be from the controls of

ISO 27002 if the institute is planning to get ISO 27001 certification. In general, the academic institutes will not require the following clauses from ISO 27001 standard.

Table 3.1: Non-Applicable ISO 27001 Clauses for Academic Institutes

Sr. No.	Clause	ISO27001 Control	Description
1	A.10.2.1	Service delivery	It shall be ensured that the security controls, service definitions, and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.
2	A.10.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
3	A.10.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
4	A.10.9.1	Electronic commerce	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
5	A.10.9.2	On-line transactions	Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
6	A.11.7.2	Teleworking	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.
7	A.12.5.5	Outsourced software development	Outsourced software development shall be supervised and monitored by the organization.

3.2.3 Phase 3:

This is a long term phase, effectiveness of controls is monitored to mitigate the identified risks. Frequent internal audits helps the institute to decide whether it is ready for certification or not. Then the external certification body performs audits and checks the ISMS of the institute for compatibility with any international standard. However, according to the proposed ISMS academic institutes may certify against ISO 27001. Since, ISO 27001 is a management standard that focuses on ISMS, policies and procedures and shows other entities in the market that this organization is competent in the information security area, thus, its certification helps to make sure that right people, processes, procedures and technologies are in place to protect information assets.

The pictorial representation of the proposed framework is shown below:

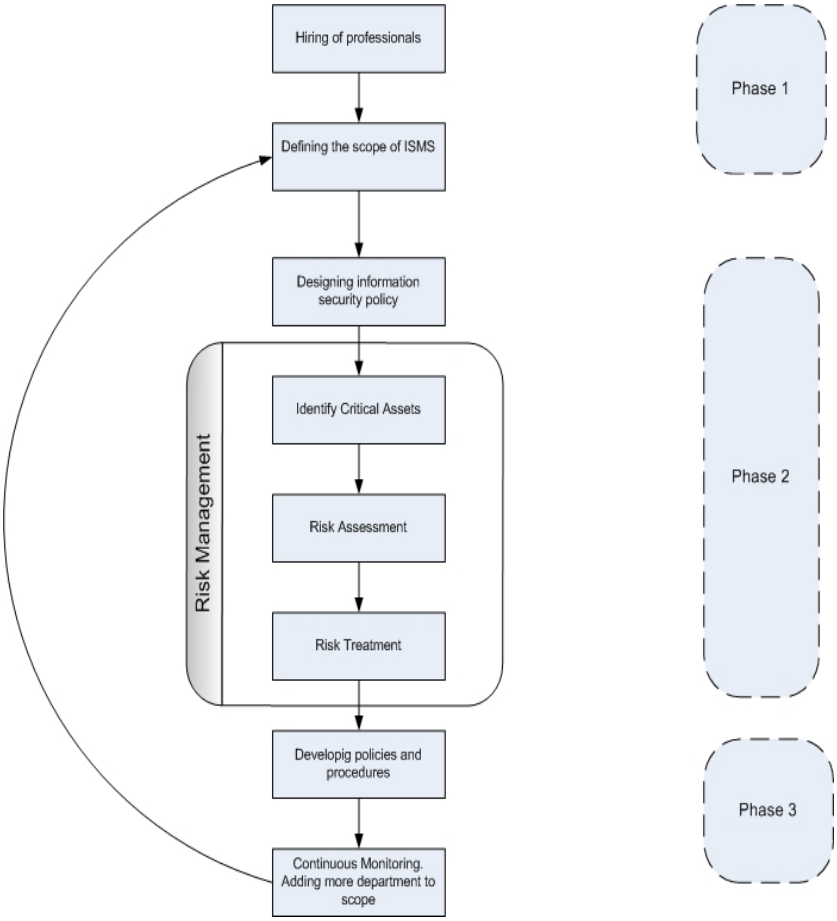


Figure 3.2: Graphic Representation of Proposed Framework

During the whole process of ISMS implementation, full support of management will be required.

Keeping in view the above methodology, MIS cell of Military College of Signals is taken as a case study whose risk assessment is performed.

Chapter 4

4. MIS CELL – A CASE STUDY

4.1 Overview

Military College of Signals (MCS), a co-educational and constituent Campus of National University of Sciences and Technology NUST, is dedicated to advancing knowledge and educating students in science and technology. Management Information System (MIS) cell was raised under Computer Science Department to provide IT services to management, faculty, staff and students in order to support them in managing, teaching, learning, and research. To achieve these goals, several tasks were carried out by MIS cell in the past:

1) Laid robust optical fibre backbone infrastructure covering college's campus, faculty accommodations, hostels and officer's mess.
2) More than 100 network switches has been installed to serve over 1000 nodes across campus, residence, hostels.
3) Wi-Fi has been deployed across the college's campus to provide internet services.
4) Indigenous designed and developed software applications for support of administrative activities, such as Electronic Mail System (eMS) for implementing paperless eOffice, Resource Information and Management System (RIMS) for managing HR data of faculty, students and staff.
5) Designed and developed software applications to support academic activities, such as Students' Attendance Management System (SAMS), Computer-Aided Student Evaluation (CASE) for online examination, Result Management System (RMS) for managing students' results, College Information system (CIS) for training management (see *Appendix A*).

6) Customized open source CMS systems to implement Learning Management System (LMS) and Online Library Catalogue (KOHA).[2]

7) Designed and developed college's website.

8) Provided IT support services in organizing conferences, seminars and workshops.

MIS cell provides internet and intranet services. Since MCS is a one of the most prominent education institutes in the country, therefore faculty and students are provided by an extensive access to internet for their Research & Development and studies. Following network devices are engaged in the process3:

1) NAYATel ONT
2) Media Converter for SCO Connectivity
3) 3Com Switch
4) Cisco 2811 Router
5) SonicWall 4500

Given below is the graphical form of whole scenario:

[2] To find the objectives of each module, please refer to *Appendix A*

[3] For description and function of each network device please refer to *Appendix A*

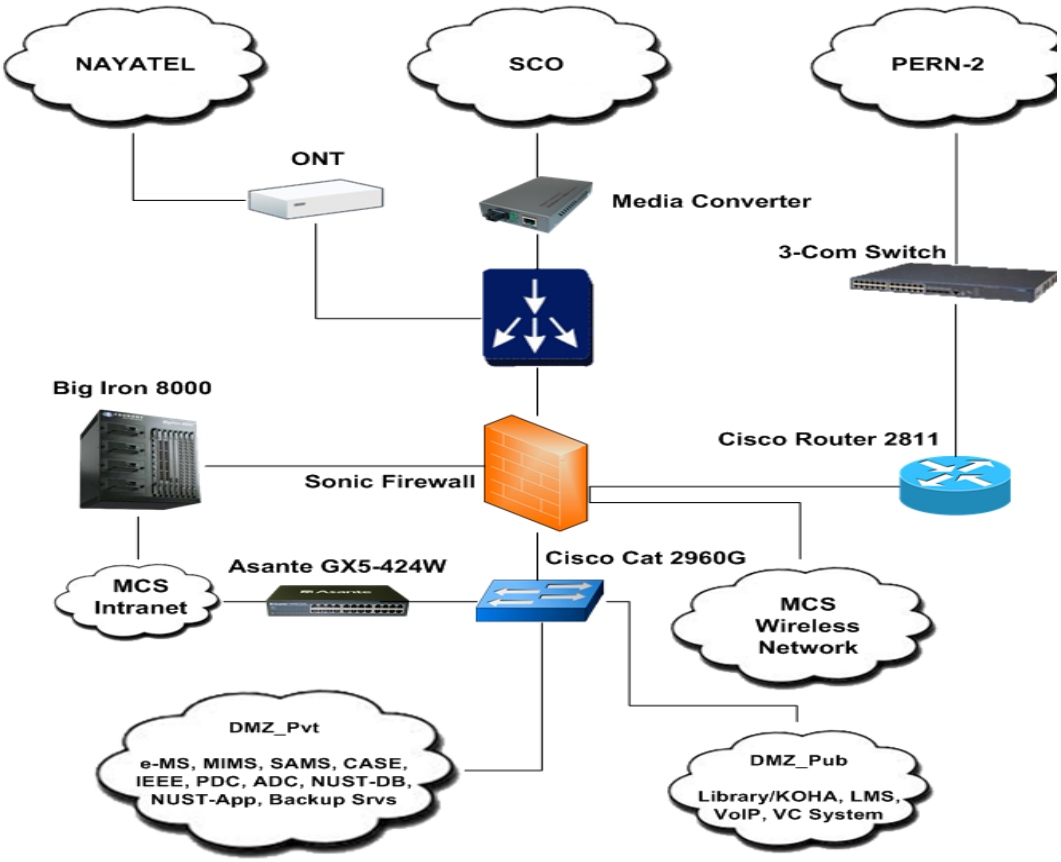


Figure 4.1: MIS Cell Internet Map

4.1.1 Existing Organizational Structure of MIS Cell:

MIS cell has a highly complex and resource rich computing environment, without which the college simply could not achieve its mission. The management structure is not that complex. The central IT organization manages the network infrastructure and other computing services.

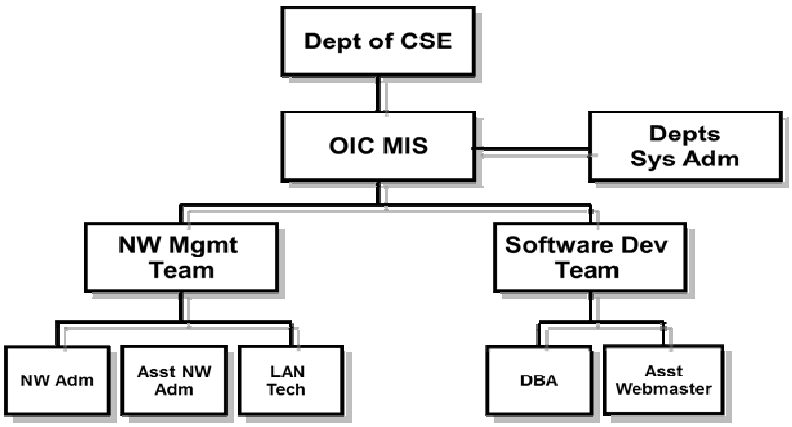


Figure 4.2: MIS Cell Organogram

The Management Information System (MIS) cell was raised under the department of CSE. The Head of MIS cell is OIC. System administrator reports to OIC MIS Cell. There are two system administrators in MIS cell. Under the network management team, there is one network administrator, one assistant network administrator and one LAN technician. And under the software development team, comes the one database administrator (DBA) and one web developer. Besides above, there are also 1 lab assistant, 1 lab attendant, 1 supervisor and 1 signalman.

4.2 Proposed ISMS Framework for MIS Cell

4.2.1 Phase 1:

In order to implement ISMS, certain new posts were suggested in chapter 3 which will help the college in implementing ISMS. The new posts suggested include posts of, Chief Information Security officer (CISO), Information Security Officer (ISO), Internal Auditor and an Information Security Management-Task Force (ISM-TF) team which may include a member of HR, CISO, OIC MIS Cell, a Network / System admin, and any other member deemed necessary as per higher management. The organizational structure will then become:

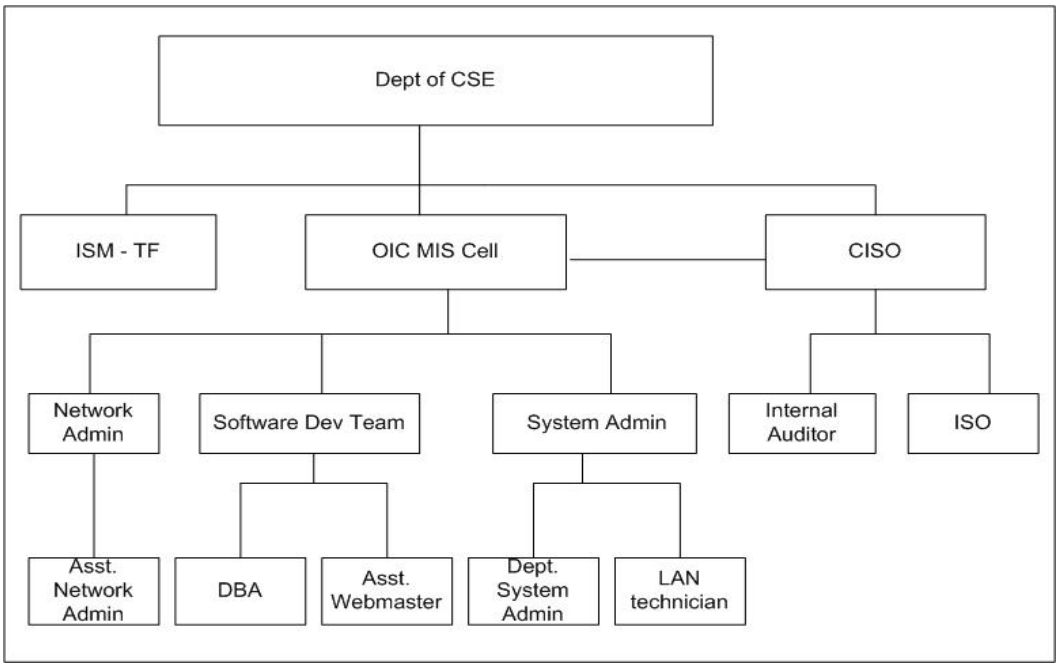


Figure 4.3: MIS Cell Proposed Organogram

4.2.2 Phase 2:

Risk management is performed in phase 2. Following steps are followed for this process:

1) Asset Identification
2) Risk Assessment
    a) Asset valuation
    b) Threat identification
    c) Vulnerability assessment
    d) Probability of risk
    e) Impact of risk
    f) Risk valuation
3) Risk Treatment

These stare explained below:

1) Asset Identification

For MIS Cell risk assessment, following assets have been considered:

a) People: include system administrators, network administrators, OIC, database administrators, LAN and system technicians.
b) Servers: include MIMS, e-MS Server, KOHA/LMS, NUST Database Server, NUST Application Server, ValueNAS.
c) End point devices: include desktops and laptops.
d) Network devices:include firewall, routers, switches, load balancer, media convertors.

Complete Asset Inventory List is given at A*ppendix A.*

2) Risk Assessment

a) Asset Valuation:

Value of each asset is determined based on confidentiality, integrity and availability. For MIS cell's assets, these are defined as:

i) ***Confidentiality***of Information Assetdetermines the impact of unauthorized disclosure of information that was confidential. The criteria set for this is:

Table 4.1: Confidentiality Criteria

Criteria	Meaning	Numeric Value
Low	The impact of unauthorized disclosure of information cannot harm to the organization	1
Medium	The impact of unauthorized disclosure of information can cause limited harm to the organization	2
High	The impact of unauthorized disclosure of information can cause severe damage to the organization. So it is highly sensitive	3

ii) By ***Integrity***of information asset, it means if integrity is not restored, the use of contaminated data could result in inaccuracy, fraud, and incorrect decisions. The criteria set for this is:

Table 4.2:Integrity Criteria

Criteria	Meaning	Numeric Value
Low	Minimal impact on business	1
Medium	Significant impact on business	2
High	Unacceptable	3

iii) ***Availability*** of Information assetdetermines that if data is unavailable to end users organization's mission may be affected. The criteria set for this is:

Table 4.3:Availability Criteria

Criteria	Meaning	Numeric Value
Low	Minimum impact on business if asset is not available for 1-3 hours	1
Medium	Significant impact on business if asset is not available for 4-8 hours	2
High	Asset is required for 24x7 basis	3

Now after determining the C, I, A values of each asset, the value of asset is determined by using the following formula:

$$\boldsymbol{AssetValue\ (V) = C * I * A} \qquad \textit{(3.1)}$$

According to above criteria minimum asset value will be (1*1*1) = 1 and maximum asset value will be (3*3*3) = 27. Thus Asset valuation matrix will be:

Table 4.4: Asset Valuation Matrix (V)

Qualitative Value	C*I*A	Asset Value (V)

Low	1 - 9	1
Moderate	10 - 18	2
High	19 - 27	3

After calculating the value of asset (V), these assets are classified as insignificant, moderate and important.

b) Threat Identification:

The threats associated with each asset are identified. These threats are categorized into:

i) Physical threat (theft, misuse of system, power failure/fluctuation etc.)

ii) Environmental threat (fire, water, cooling etc.)

iii) Cyber threat (DOS, hacking, illegal of use of software etc.)

iv) Insider threat (disgruntled employee, etc.)

c) Vulnerability Assessment:

Identify the vulnerabilities that can be exposed by the identified threats. They are categorized as follows:

i) Technology vulnerability (operating system weakness, network equipment weakness etc.)

ii) Configuration vulnerability (unsecured user accounts, misconfigured internet services, unsecured default settings, misconfigured systems etc.)

iii) Security policy vulnerability (lack of written security policy, illegal use of software, untrained staff etc.)

The table 4.5 shows the basic vulnerabilities and risk associated with each identified threat:

Table 4.5: Threat, Vulnerability & Risks

Threat	Vulnerability	Risk
Fire	Inadequate fire detection equipment	Fire can destroy the asset making it unavailable for

	Inadequate fire suppression equipment	the users
Air-conditioning failure	Inadequate environmental protection	overheating of data center may lead damage to physical assets & disability of operational & business services
	Inadequate equipment maintenance	
Denial of service attack	Operating system vulnerabilities	DOS attacks will result in the unavailability / modification / confidentiality breach of services to the legitimate user
	Inadequate anti-malware software	
	Inadequate anti-malware software updating	
	Inadequate control downloading & using	
	Inadequate control of internet usage	
	Inadequate control over system access	
	Inadequate security awareness & trainings for staff	
	Inadequate configured & maintained firewall	
	Unauthorized equipment connected to server	
Software failure	Inadequate application controls	Services associated with asset will become unavailable
	Inadequate authorization & configuration changes	
	Inadequate change control	

Human Error	management	Accidental human error can make critical services or data inaccessible, or can create vulnerabilities which can help in hacking, activate unwanted services, data theft/loss.
	Inadequate or incorrect assignment of responsibilities	
	Inadequate security awareness & trainings for staff	
	Inadequate separation of test & operational facilities	
	Over-reliance on key staff/ lack of delegation	
Malicious Code	Inadequate anti-malware software	Asset can stop functioning & associated services can be stopped.
	Inadequate anti-malware software updating	
Hacking	Failure to apply relevant software patches	Hacking is associated with numerous risk e.g. Unauthorized external & internal access, data theft,
	Inadequate anti-malware software	
	Inadequate anti-malware software updating	
	Inadequate control downloading & using software	
	Inadequate control over system access	
	Inadequate security awareness & trainings for staff	
	Inadequate configured & maintained firewall	
	Mixing of tests, development & operational facilities	
	Unauthorized equipment connected to server	

	Unprotected public network connections	data loss, service unavailability, misuse of services, unauthorized access through social engineering
	Default factory settings not changed	
	Inadequate analysis of network logs	
	Inadequate arrangement of removing access rights	
	Inadequate change control management	
	Inadequate control of use of system utilities	
	Inadequate identification & authorization	
	Inadequate wireless network security controls	
Power supply or fluctuation	Inadequate UPS	Asset can stop functioning & associated services can be stopped.
	Power fluctuations / outages to areas	
Illegal use of software	Inadequate authorization for configuration changes	Penalization by law enforcement agencies
Theft	Inadequate physical security	Data residing in the asset will be compromised
	Unmotivated or disgruntled staff	
Insufficient or untested backups	Inadequate back-up facilities	In case of disaster, failure to continue with business continuity process
	Inadequate back-up testing	
System misuse		

	Failure in change management	Misuse of a system deliberately or accidently will result in compromising of data.
	Inadequate arrangement of removing access rights	
	Inadequate authorization for configuration changes	
	Inadequate control over system access	
	Inadequate security awareness & trainings for staff	

d) Probability of Risk:

Estimate the chance of occurrence or probability of the risk (P). The scale set for probability of occurrence is given in table 4.6:

Table 4.6: Probability of Risk (P)

Quantitative value	Qualitative Value	Description
1	Rare	Once in a year
2	Periodic	Once in a quarter
3	Regular	Once in a month
4	Frequent	Once in a week

e) Impact of Risk:

Estimate the impact of risk on business value (I). The scale for Impact of risk is given in table 4.7:

Table 4.7: Impact of Risk (I)

Quantitative value	Qualitative Value	Description
1	Insignificant	Effects can be ignored
2	Minor	Can effect operations of team/ department
3	Moderate	Can effect internal operations of MCS
4	High/ Catastrophic	Can effect business operations and

		goodwill of MCS involving legal consequences

f) Risk Valuation:

Assess the level of risk with the help of following formula:

$$\boldsymbol{Risk\ Rating\ or\ RiskValue\ (R) = V * P * I} \qquad (3.2)$$

The scale for Risk value is given in table 4.8:

Table 4.8: Risk Rating(R)[4]

Risk Rating	Qualitative value	Description
1 - 12	Low	Treatment can be delayed
13 – 24	Medium	Treatment required but does not need immediate action.
25 - 36	High	Can have severe impact if not treated immediately
37 – 48	Critical	Can effect MCS operations and immediate treatment is needed

3) Risk Treatment

The following steps are taken in the risk treatment phase:

a) Description of currently deployed measures for removing the vulnerabilities and reducing the risks

b) Select control objectives and controls for the treatment of risks from ISO 27002:2005

c) Define the level of Risk Acceptance and obtain management approval

d) Obtain management approval for proposed residual risks.

[4] Risk treatment is done against assets whose risk ratings are critical and medium

4.3 Risk Management – Examples

1) Servers:

Take the case of asset server **MIMS.** Following threats have been identified: fire, air conditioning failure, denial of service attack, hacking, human error, malicious code, power supply failure/fluctuation, software failure, system misuse, theft, illegal use of software and insufficient or untested backups. After this, there is a column for asset value. Asset value is calculated according to C, I, A values of asset discussed in chapter 3. Then comes the "IMPACT" column. It is calculated by assuming that if the identified vulnerability is exploited, what would be its impact on MCS. The scale is set and already discussed in chapter 3. For instance, the threat is "hacking" and the vulnerability is "failure to apply relevant software patches". If this vulnerability is exploited it would result in data leakage, data corruption or data theft. If any of this happens it would leave a great impact on MCS reputation as well as its operation, or MCS might face legal consequences. Thus its value is high. It should be noted that the impact is calculated by assuming if no current control is applied on that vulnerability. Similarly discussing another threat "Fire". Fire can result complete destruction of asset. If the vulnerabilities are "inadequate fire detection equipment" (like smoke detectors) or "inadequate fire suppression equipment" (like fire extinguishers are expired or not available), the fire can cause great harm and its impact would be high on MCS. It would not only destroy the asset making it unavailable for the users but also the news would become the talk of the town effecting the reputation of MCS. The next column is "PROBABILITY" of occurrence of exploiting that vulnerability. The scale is already discussed in chapter 3. Taking the same example discussed above, the probability of occurrence of exploiting the vulnerability "failure to apply relevant patches" is high because vendors provide the relevant patches for a loophole but if custodian fails to apply that patch in time, the chances of exploitation becomes high. Similarly for a fire case, the likelihood of this asset to catch a fire is low because the cooling system inside the data centre is appropriate. Then comes the column for "RISK VALUE". Risk value is calculated by multiplying the values of asset, impact, and probability and then "RISK LEVEL" is

assigned according to the scale discussed in table 3.7 in chapter 3. For instance, against the vulnerability of “failure to apply relevant patches” for threat “hacking”, the risk value is **36** and according to table 3.7, the risk level becomes **High.** Similarly for vulnerability of “inadequate fire detection equipment” and “inadequate fire suppression equipment” of threat “fire”, the risk value is **24** which is **Moderate** according to scale of table 3.7. It should be noted that Risk value is a quantitative value and Risk Level is a qualitative value. The next column is of “CURRENT MEASURES”. Current measures are those measures which are taken by the custodian already to avoid that vulnerability. The current measures are determined by taking interviews of the custodian and where necessary questionnaires were filled. Thus, for “Failure to apply relevant patches” vulnerability, the current measure is “windows update service is enabled” which is automatic. For “inadequate fire suppression equipment” and “inadequate fire detection equipment”, the only current measure is the “presence of fire extinguishers” in data center. After current measures column, there is a column of “ISO 27001 CONTROL”. This is the column where I’ve suggested the control for the vulnerability/threat from ISO 27001 standard. Thus for “failure to apply relevant software patches, three controls were suggested: **“A.12.4.1 Control of operational software”**. This control says there shall be procedures in place to control the installation of software on operational Systems. Second control is “A.12.5.1 Change of control procedures”. This control says that the implementation of changes shall be controlled by the use of formal change control procedures. And third is **“A.12.6.1 Control of technical vulnerabilities”** which says timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. For “Fire” threat, the control suggested is **“A.9.1.4. Protecting against external & environmental threats”** which says Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied. The last column “REASON/COMMENTS” is optional. However it is used whenever it isestablished that the current measure is not enough or appropriate to protect the asset. Like in case of fire, it is found that in the data

center, no smoke detectors are installed, there is improper & insufficient earthing& cabling, lose power connections and power distribution points.

2) Network Devices:

Network devices include router, switches, firewall, load balancer, media convertors. Although they don't have any critical or sensitive data residing on them but they are as important as the servers are. For instance, the significance of firewall can be judged from the fact that it splits the network in two which makes it easy to decide which network traffic is to be trusted. So a firewall SonicWall 4500 is placed between the ISP's internet and internal network. This is the first defense of security. So based on its C, I, A, it is the critical asset of MIS cell. If the firewall is misconfigured, and the attacker finds this vulnerability and exploit it, it will open the gates for numerous attacks like SQL injection, cross-site scripting, port scanning, e-mail spams, DOS attacks breaching the servers and endpoints. These methods can harness user credentials, sensitive information (like personal data and academic data of students, faculty, staff), and intellectual property to name a few. This would leave a great impact on the institute. So its impact value is 3 (according to table 4.7). So the network administrator must be properly trained and expert on firewall handling and configuration. The probability of occurrence of the risk if this vulnerability (i.e. **inadequate configured and maintained firewall**) is exploited is **3** (according to table 4.6). So the overall risk rating is **27**making it a "**medium**" risk level (according to table 4.8). However, it is found that the firewall is "**properly maintained and configured**". So, the control suggested from ISO 27001 is "**A.10.6. Network Security Management".**

Similarly, switches are as important as other network devices. The switches help to create VLANs. VLAN has the same characteristics as a physical Local Area Network (LAN). It is a separate IP sub-network which letsseveral networks and subnets to reside on the same switched network and can be designed department-wise, function-wise, or protocol-wise, allowing for a smaller layer of granularity. A VLAN cannot communicate directly with another VLAN. For VLANs to communicate with each other the router or layer 3 switching is required. So, layer 3 switch BigIron 8000 is installed. Its confidentiality is not

that important as that of availability. However, based on its C, I, A this asset is also critical and its value is 3. VLANs are configured on this switch. Thus allowing sensitive or confidential data to transmit through the network decreasing the risk that users will gain access to data that they are not authorized to see. However, if the "default factory settings" are not changed, attacker will exploit this vulnerability and generate attacks like spanning-tree attack, MAC table spoofing, ARP attacks, VLAN hopping etc. If these attacks are successful, the impact on the institute will be significant. It will affect the operations of MCS. Thus the value is **3** (according to table 4.7). The probability of occurrence of this risk is **3** (see table 4.6), making the risk value to **27** (Medium) according to table 4.8. The ISO 27001 suggested control is **A.10.6.1 Control on Technical Vulnerabilities.**

Exactly the same method has been followed so for all servers, laptops/desktops and other network devices. The risk assessment sheet is attached in the next page. Complete assessment of controls (current security controls) on each asset is mentioned in the risk assessment sheet under column "Current Measures"[5].

[5] Refer to risk assessment sheet for present controls and ISO 27001 controls.

Table 4.9: Risk Assessment Sheet

4.4 Formation of SOA

Forming a statement of applicability is one of the important and basic requirement of ISMS. It is the list of controls that were adopted and not adopted with complete justification and reference. Two types of SOA are developed during ISMS implementation. Initial SOA is developed in the PLAN phase, which suggest the list of ISO 27001 controls that should be implemented and not implemented with justification, keeping in view of risk assessment and its treatment. Management approval is needed in this phase. The Final SOA is developed in Do phase. When the appropriate controls are implemented against the risk the documented reference of that implemented control is mentioned in the SOA which was developed in plan phase. Thus we can say that SOA is the connection between risk assessment and risk treatment and the implementation of organization's information security. It is a proof that management has approved or disapproved this particular control for the risk and it is documented.

ISO 27001 has 11 control domains with 133 sub-controls. Each domain has its own objectives which are briefly described below:

1) **Information Security Policy:** This domain specifies that in order to clarify thedirection of, and support for, information security, top management should define a set of policies according to the business requirements. So preparing an information policy document is mandatory here.
2) **Organization of Information Security:** This domain provides clear direction and visible management support within the organization and information security responsibilities for internal and external parties of organization.
3) **Asset Management:** To achieve and maintain appropriate protection of organizational assets, and inventory of information, software and physical asset is maintained, information should be classified and information handling procedures should be defined.
4) **Human Resource Security:** This domain specifies the need of human resource security. Background verification checks on all candidates for employment,

signing the confidentiality/ non-disclosure agreements, giving information security trainings and taking disciplinary actions against security violations are the key security features in this domain.

5) **Physical and Environmental Security:** Physical protection of premises/ facilities against natural disasters and communication interception are covered in this domain.

6) **Communications and Operations Management:** Operating procedures for secure and correct operation of information processing facilities, detection and prevention of malicious software, data backup, network, email, portable media and disposal management procedures are defined here.

7) **Access Control:** This domain covers the access control to information by keeping in account the user registration/ de-registration process, password controls, user access review, audit logging and remote access control

8) **Information Systems Acquisitions, Development and Maintenance:** To ensure the security as an integral part of information systems, data validation, message authentication, cryptography management, control over testing data, prevention against covert channels are covered in this domain

9) **Information Security Incident Management:** Incident prioritization and classification, incident reporting, incident escalation procedures are covered in this domain.

10) **Business Continuity Management:** In this domain business continuity framework and plan is defined.

11) **Compliance:** To avoid breaches of any law, regulatory or contractual obligations procedures are defined under this domain.

The initial SOA has been developed after the risk assessment. It is attached in the end. The first column is “ISO 27001 Clause” which shows the clause number of standard. The second column is “ISO 27001 Control”, the control that is selected. The third column is “Applicability”. It shows whether the control is applicable, not applicable or partially applicable. Fourth column is of “Control objectives” of that control. And fifth column is

of “statement of applicability and non-applicability” which justify why this controls is or not selected. For instance, in the SOA sheet, the first column is taking ISO 27001 clause “*A.5.1.1*” as an input. In second column ISO 27001 Control, the name of A.5.1.1 control “*Information security policy document*” is written. Whether the control is applicable or not is selected in Applicable column. It is “*Applicable*”. Then, the fourth column is the control objective, which in case of A.5.1.1 is “*An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties*“. Then in the statement of applicability/ non applicability column, this control is justified by stating “*it defines the ISMS framework*”.

For another control “*A.5.1.2*” this control is also “*applicable”* and justified by stating that “*to ensure security requirement of business is effectively evaluated and monitored*”. The clause “*A.10.9.1*” “*Electronic Commerce*” is “*not applicable*” and is justified by stating that “*MIS Cell is not dealing with any buying and selling of the products*”

SOA is a public document which means it is provided on demand but justifications of control or how the control is implemented should not be too clear so that it may not help anyone with false intensions to learn the security controls of the organization.The generalized SOA for academic institutes are developed. *See Appendix B.*

Table 4.10: Statement of Applicability

Chapter 5

5. CONCLUSION

5.1 Introduction

This research was conducted to carry out the risk assessment for educational institute to implement ISMS. MIS cell of Military College of Signals was taken as a case study and ISO 27001 was selected as a standard to implement ISMS. During the procedure, it was analysed that one can simply attain the standard by limiting the scope of ISMS. So, a security plan should be developed first by adopting the "best practices" for information security, and certify one department (i.e. MIS Cell) with ISO 27001. Once this department, successfully complete its external audit, the university should add different departments to the scope for certification. It is an ongoing process. So develop a "phase-incremental approach" for this purpose.

Risk assessment was the prime objective of the thesis. Risk assessment has been carried out on MIS cell. All the required documents for a PLAN phase of implementing ISO 27001 have been developed and provided. It is necessary to adopt all those controls discussed in SOA to certify for ISO 27001 standard.

Although in this research work ISO 27001 is taken as a standard to implement but it has a weakness. It does not describe what type of tool or device is to be used as a control or how to configure it to achieve the best level security. For instance, it says use anti-malware tool to protect from malicious components, but it doesn't specify what anti-malware tool is the best. An institute can attain ISO 27001 certification even by using a freeware version of anti-virus or spend some money in buying a licensed antivirus. Similarly it doesn't describe how to configure a firewall. So the institute has to define it by itself keeping in view the incidents that could happen. Along with risk management there are certain other practices which must be adopted to provide security to the information assets by educational institutes. These are discussed below:

1) Centralized Anti-Malware Tool:

A centralized anti-malware tool needs to be installed and IT department should be the custodian of that tool. Updates are pushed automatically to clients endpoints from the server rather than a lab attendant go and install manually on every system.

2) Network Access Control (NAC) System:

Network Access Control (NAC) systems will allow authorized systems, which are properly configured, to connect to the network. If a new system is introduced in the environment, NAC will identify it. The system will not be given access to the network unless it complies with information security policies of the organization. For instance, endpoint device protection policy that includes installation of antivirus, system updates, security configurations etc. Once the policies are enforced and the system complies, it can access the network and the internet. NAC can also provide role-based access mode in which access is given according to the role of a person.

3) Patch Management:

Vulnerabilities in operating systems (OS) and software help an attacker to compromise the systems. So their respective vendors release patches for these security loopholes and vulnerabilities. Thus, all the software and operating systems should be timely patched and this should also be centralized.

4) Data Protection:

Academic institutes have personal information of faculty, staff, students, alumni, and researchers (e.g. CNICs, date of birth, financial and medical information, grades, telephone numbers, and permanent addresses). Furthermore, these institutes conduct research and development for all technology innovations in the country. In order to prevent unauthorized access and modification, staff, faculty and students' bio data, records, results or other restricted data should be saved in encrypted form or in encrypted containers.

5) Use of Domain Emails:

All the faculty members, staff and students are required to use institutes' assigned domain emails rather than using any other public accounts for communication. This will help to cater the problem of repudiation and misuse of e-mail IDs.

6) Log Management:

An attack may go unnoticed if logs are not recorded and protected properly. So, logging should be activated on every machine and logs are sent to centralized log server. For this purpose, security information and event management (SIEM) tools should be deployed and firewalls, proxies, and VPNs all should be configured for verbose logging.

7) Control of network ports, services and protocols:

During the software installation many services are also installed and turned on without informing the user that a services has been enabled. Attackers search remotely accessible networks and scan for such services or open ports and exploit them. So administrators make sure that any service which is not needed is disabled or uninstalled. Perform port scan on regular basis. Create a baseline for all services, protocols and ports that are enabled and compare the scanned result to that baseline. This will help to identify the unnecessary ports, services that are opened without the consent of administrators.

8) Control Use of Administrative Privileges:

Use of administrative accounts should be on required basis. Monitor the activities of administrators as well. For this purpose, tools are available in the market. The passwords should be complex and change the regularly. Make sure that administrator accounts are used solely for administrative activities not for browsing, personal internet activity, reading mail etc.

9) User Account Monitoring:

Ensure all the accounts comply with university's password policy. Review all the accounts and disable the accounts that are no longer in use. Revoke the rights to access the accounts on employee's termination and deactivate the accounts of students who pass out from the institutes. The attempt to access the disabled accounts should be monitored regularly through audit logging.

10) Incident Response Management:

Design a proper incident response procedure. When an incident is occurred, it should be properly documented including the steps taken for incident handling. Assign roles and responsibilities for computer as well as network incident handling. Develop an incident response team.

5.2 Future Work

Breaking a large institute into smaller units and limiting the scope of ISO 27001 and then with the passage of time broadeningof scope by adding one department every yearcan help achieve the standard levels. Risk Analysis for MIS Cell has been carried out during this research. In order to certify MIS Cell with ISO 27001, all the controls suggested in SOA (seechapter 5) must be implemented along with proper documentation. This work can be extended by carrying out risk assessment of all the departmentsseparately, formulating the information security policies and implementing them in the university at largeand evaluating the effectiveness of all the implemented controls in the later stages.

Besides this, another area of future research can involve focusing on assessing the types and volume of illicit and cyber-criminal activities occurring in academic institutes. These cyber-criminal activities (e.g. identity theft, denial of service attacks, intellectual property theft, scam, penetration into the government and private organization's networks) are increasingly propagating by computers infected by malicious software and since the academic institutes are considered more vulnerable to these activities, little empirical research has been conducted on this issue.

Another area of future research can bepractically determining the impact of policies and practices on information security in academic institutions. This will include empirically assessing attacks to and originating from academic institutions, measuring the impact of implemented security controlson network, identifying the obstacles and facilitators toimplement the security controls in an academic environment; and/or providing clear direction for next steps in security policy and best practices.

5.3 Conclusion

To conclude, information security management framework is essential for the overall security of data in the academic institutes. Academic institutions impend lopsided threat to public safety,as they are perceived of being the weakest link due to the profligate bandwidth usage and erratic security practices. This feature burgeons illicit activities via internet and increases inducement of perpetrators to incline towards softer targets i.e. academic institutions. All of our systems are inter-connected and problem in one sector directly affectother sectors in the country.So defining a sound information security management system is the responsibility of universities' management. Hence, the practices discussed above must be mature enough for achieving standard level.

6. BIBLIOGRAPHY

[1] Basie Von Solms, Rossouw Von Solms, "The 10 deadly sins of Information Security Management", Computer & Security, Volume 23, Issue 5, July 2004.

[2] M. James, "Information Engineering, Prentice Hall, 1989.

[3] S. K. Leem Choon Seong, "Introduction to an Integrated Methodology for Development and Implementation of Enterprise Information Systems", Journal of Systems and Software, Volume 60, Issue 3, pp. 249-261, 2002.

[4] NIST, An Introduction to Computer Security, The NIST handbook, 1995.

[5] Rex K. Rainer, Charles A. Synder, Housten H. Carr, "Risk Analysis for Information Technology",Journal of Management Information Systems, Volume 8, No.1, 1991

[6] W. Ron, EDP Auditing: Conceptual Foundations and Practice, McGraw-Hill, 1988.

[7] Gerald V. Post and J. David Diltz, "A Stochastic Dominance Approach to Risk Analysis of Computer Systems", in MIS Quarterly, 1986.

[8] R. Hammond, Improving Productivity Through Risk Management,Handbook of MIS Management, 2nd ed., pp. 655-665, 1988.

[9] Rex K. Rainer, Charles A. Synder, Housten H. Carr, "Risk Analysis for Information Technology," Journal of Management Information Systems,Vol. 8, No.1, 1991.

[10] J. Newton, "Developing and Implementing an EDP Disaster Contingency Plan for a small national bank," Unpublished Master thesis, 1987.

[11] Sangkyun Kim and Choon Seong Leem, "An Information Engineering Methodology for Security Strategy Planning", Computational Science and its Applications - ICCSA, Volume 3043, pp. 597-607, 2004.

[12] M. Lin, Q. Wang, J. Li, "Methodology of Quantitative Risk Assessment for Information System Security," Computational Intelligence and Security, Volume 3802, pp.526-531,2005.

[13] Choon S. Leem, Sangkyun K. and Hong J. Lee "Assessment Methodology on Maturity Level of ISMS",*inProc.9th international conference onKnowledge Based Intelligent Information and Engineering Systems*, 2005.

[14] HeruSusanto, Mohammad Nabil Almunawar, Yong Chee Tuan, "Information Security Management System Standards: A Comparative Study of Big Five," International Journal of Electrical & Computer Sciences, Volume 11, No. 05, 2011.

[15] "ISO" [Online]. Available: Http://www.iso.org/iso/about/discover-iso_isos-name.htm.

[16] Abdulkader Alfantookh, "An Approach for the Assessment of the Application of ISO 27001 Essential Information Security Controls", King Saud University, 2009.

[17] "PCI Security Standard Council," [Online]. Available: https://www.pcisecuritystandards.org/security_standards/index.php.

[18] Basie von Solms, "Information Security Governance – Compliance Management vs Operational Management," Computer & Security Journal,Elsevier, Science Direct, 2005.

[19] "Overview on COBIT," [Online]. Available: http://www.benchmarklearning.com/COMMUNITIES/ITIL/cobit.aspx.

[20] "Introduction to ISMS-ISO 27001," [Online]. Available: http://e-learning.s3.amazonaws.com/chapter-2/introduction-to-ISMS-ISO27001/introducton-to-ISMS-ISO-%2027001.html.

[21] Steffani A.burd, "The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice",document no. 215953,2005.

[22] D. DesPlanques, "Information Security Policy development for Institutions of Higher Education", Regis University, School for Professional Studies: MSCIS thesis.

[23] D. S. Bhilare, A. K. Ramani, Sanjay Tanwani, "Information Protection in Academic Campuses: A scalable Framework," Journal of Computer Science, Vol. 4, Issue. 10, pp. 864-870, 2008.

[24] “HIPPA Security and Privacy,” [Online]. Available: http://www.hipaasecurityandprivacy.com/2009/12/internet-security-breach-found-at-ucsf.html.

[25] “University of California, Santa Cruz,” [Online]. Available: http://its.ucsc.edu/security/breaches.html.

[26] “PC World,” [Online]. Available: http://www.pcworld.com/article/125662/article.html?page=1.

[27] “Daily times. pk,” [Online]. Available: http://www.dailytimes.com.pk/default.asp?page=2011\08\16\story_16-8-2011_pg11_9 .

[28] I. Application Security, “An Examination of Database Breaches at Higher Education Institutions,” pp. 1-6.

[29] [Online]. Available: http://www.innova-sa.eu/security/information-security-management-isms.html.

[30] “Manchester University, UK,” [Online]. Available: http://www.its.manchester.ac.uk/secure-it/policies.

[31] U. S. C. I. S. A. (UCISA), USCISA Toolkit: Information Security, 3.0 ed., UCISA, 2005.

[32] I. 27005, Information technology — Security Techniques — Information Security Risk Management, 2nd ed., 2011.

7. APPENDIX A

ASSET INVENTORY LIST

1) Servers

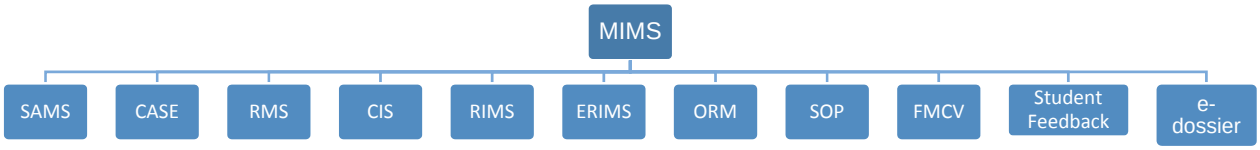
MIS Cell has following servers installed:

1) MIMS Server
2) e-MS Server
3) KOHA/LMS Server
4) NUST Database Server
5) NUST Application Server
6) ValueNAS(not operational now, instead SAN is being used)
7) 3 Proxy Servers
8) Radius Server
9) 2 PDC
10) ADC

Significance of each server is given below:

1) <u>MIMS Server</u>

MIMS server is a web based system, programmed in C# language with MS SQL server 2008 database at the backend. It has 11 modules.



The objective of these eleven modules is given below:

1.1) Computer Aided Software Evaluation (CASE): To automate the student evaluation system.

1.2) Student Attendance Management System (SAMS): To automate student attendance and provide report for decision making.

1.3) Result Management System (RMS): To automate efficient processing of results for combat wing.

1.4) College Information System (CIS): To perform training management and activities, to create courses and add subjects.

1.5) Resource Information and Management System (RIMS): To manage HR (both employees and students) related data.

1.6) Equipment Repair and Inventory Management System (ERIMS): To automate the work order flow and record the history of equipment purchased,

1.7) Online Registration Module (ORM): To register the newcomer on MIMS. (The verification of data is done by the course advisor of that class).

1.8) Standard Operation Procedures (SOP): It's a repository of SOPs.

1.9) Faculty Members' Curricular Vitae (FMCV): It's a repository of faculty members' CVs.

1.10) Student Feedback: To evaluate the instructors by the students.

1.11) E-dossier: To keep the record of students' complete bio data, academic records, research activities, achievements in extra-curricular activities, awards, warnings, medical records etc.

2) <u>e-MS Server</u>

Its purpose is to automate office correspondence and make MCS paperless campus of NUST.

3) KOHA/LMS Server

It has two modules: KOHA and LMS.

3.1) Learning Management System (LMS): To provide an application for the faculty members to upload lectures, notes and important announcements for students so that they can access them from home.

3.2) KOHA: To provide library information and management system.

4) NUST Database server

It syncs data between NUST application server and NUST HQ. It has ERP exam module. This module is used by engineering wing to conduct exams, compile results and to generate transcripts.

5) NUST Application server

It provides interface for previous server and provides integration for NUST database server and exam module.

6) ValueNAS

This server provides services to take Backup of Core Servers. Acronis True Image Server is used as Backup Taking Agent and ValueNAS is used for Storage purpose.

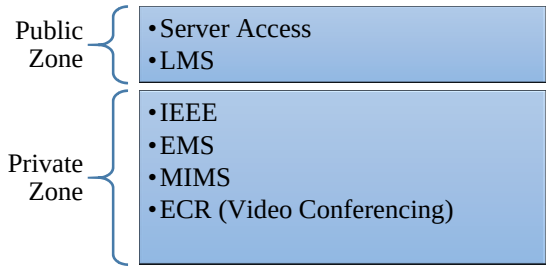
2) Network Devices

1) Firewall (1)

Device	Category	Details	Importance
Sonic Firewall 4500	Firewall	▪ 6 x GigEth Ports ▪ 1 x Console Ports ▪ 2 x USB Ports	▪ Monitoring/Logging ▪ Packet Filtering ▪ Intrusion detection &

			Prevention ▪ Security ▪ NATing ▪ VPN

Zone Defining



- To utilize its physical interfaces to maximum we use ISP-1 and ISP-2 in it

2) Firewall (2)

Device	Category	Details	Importance
Juniper NetScreen 50	Firewall	3 x FastEth Ports for ▪ Console ▪ Modem ▪ Compact Flash	Supporting device for in-depth security

- It is used for Direct Access (café 1, café 2, library)
- Max Bandwidth is limited
- No zoning as max ports of fast Ethernet are 4

- No load balancing

3) Core Switch

Device	Category	Details	Importance
Foundry BigIron 8000	Core Switch	▪ 8 x Modules available ▪ 3 x slots working with gigabit connectivity	▪ Core of the Intranet ▪ Connecting all departments/subnets ▪ Support L2/L3 functionality

- It is a Network Layer Switch
- Follows star topology
- Hub of all intranet connectivity at MCS
- If it goes down then it would result in a disaster
- IP subnet based VLANs , 19 subnets available
- Inter VLAN switching in order to segregate departments, students, etc.

4) Router

Device	Category	Details	Importance

Cisco 2811	Router	▪ 2 x FastEth ▪ 4 +1 modules available for expamsion	Providing connectivity of MCS Network to/with PERN-2

- It is connected to the PERN-2 ISP
- No backup if any problem arises with this router

5) <u>Load Balancer</u>

Device	Category	Details	Importance
TP Link – TL R488T	Load Balancer	▪ 4 x WAN Ports ▪ 1 x LAN Port ▪ 1 x Console	▪ Aggregation of multiple ISP Links ▪ Auto Fail Over Feature ▪ Individual ISP Load Balancing, allocation of Bandwidth and Load over available connections

- All ISP links are aggregated through this load balancer

6) Layer-2 Switch (1)

Device	Category	Details	Importance
3Com 4200	Layer-2 Switch	▪ 26 x FastEth ▪ 2 x GBIC (Fiber Support)	▪ Connects Fiber Link from PERN-2 to MCS Network

7) Layer-2 Switch (2)

Device	Category	Details	Importance
3Com 4226T	Layer-2 Switch	▪ 26 x FastEth	Connects: ▪ CoTEWrls (Wireless) ▪ MIS Cell Lab ▪ Server Room Systems

8) Layer-2 Switch (3)

Device	Category	Details	Importance
Cisco 2960G	Layer-2 Switch	▪ 24 x FastEth	Distribute DMZ_Pvt and DMZ_Public

9) Layer-2 Switch (4)

Device	Category	Details	Importance
Asante FriendlyNET GX5-424W	Layer-2 Switch	▪ 24 x FastEth ▪ 2 x 10/100/1000 ▪ 1 x each (SFP,minGBIC)	▪ Connects MIS Cell servers (PDC, ADC, Proxy etc) ▪ Bridge Link for MIS Cell Lab ▪ Provide uplink for few dept over FastEth ▪ Provides uplink to BigIron 8000for rest of the Intranet ▪ Provide Connectivity with SonicWall for internet access

10) Layer-2 Switch (5)

Device	Category	Details	Importance

TP Link SF 1024	Layer-2 Switch	▪ 24 x FastEth (10/100)	▪ Used in stack with Asante

8. APPENDIX B

The Following table shows the general SOA designed for academic institutes of Pakistan. The columns ISO 27001 clause, ISO 27001 Control and Control Objectives are taken from standard ISO 27001:2005 controls i.e. Information Technology – Security Techniques – Code of Practice of Information Security Controls (ISO 27002). The column "Statement of Applicability/Non Applicability" provides the justification for the controls that are applicable or non-applicable. " *

ISO 27001 Clause	ISO 27001 Control	Control Objectives	Statement of Applicability/ Non Applicability
A.5	**Information security policy**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**	
A.5.1.1	Information security policy document	An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.	It defines the ISMS framework
A.5.1.2	Review of the information security policy	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	To ensure security requirements of business is effectively evaluated and monitored
A.6	**Organization of Information Security**		

A.6.1	**Internal organization**	**To manage information security within the organization.**	
A.6.1.1	Management commitment to information security	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.	Management commitment is required for endorsing, communicating and implementing Information security policies to all concerned levels.
A.6.1.2	Information security coordination	Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job function.	Information security roles and responsibilities and Security System Procedures need to be developed to ensure that people are aware of their roles in light of Information Security requirements.
A.6.1.3	Allocation of information security responsibilities	All information security responsibilities shall be clearly defined.	Information security responsibilities should be defined for individuals and groups in the ISMS manual and their Job Descriptions.
A.6.1.4	Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be defined and implemented.	Users should be authorized to information processing facilities and privileges on the basis of their job roles and responsibilities.
A.6.1.5	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the	Service Level Agreements and Employment Contracts must include Confidentiality requirements for compliance

		protection of information shall be identified and regularly reviewed.	with Information Security requirements and all employees, contractors need to sign this confidentiality agreements
A.6.1.6	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Contact list of appropriate authorities shall be maintained.
A.6.1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Contact should be maintained with external parties such as ISPs, IT vendors and Physical security services providers.
A.6.1.8	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	ISMS-steering committee should be formed and ensure that their audit activities are independent of any internal or external influence that could affect the audit result and its integrity.
A.6.2	**External parties**	**To maintain the security of organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.**	
A.6.2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be	Risks associated with third parties including vendors shall be identified and assessed through risk management procedure

		identified and appropriate controls implemented before granting access.	
A.6.2.3	Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.	OIC, in consultation with CISO are responsible to maintain security measures in third party agreements.
A.7	**Asset Management**		
A.7.1	**Responsibility for assets**	**To achieve and maintain appropriate protection of organizational assets.**	
A.7.1.1	Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.	The inventory of Information assets shall be maintained and included in the asset valuation sheets that are part of Risk Management System
A.7.1.2	Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designated part of the organization.	ownership of asset should be clearly assigned in asset inventory

A.7.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.	An acceptable use of asset policy should be developed and communicated to users.
A.7.2	**Information classification**	**To ensure that information receives an appropriate level of protection.**	
A.7.2.1	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.	Data Classifications Procedure should be developed that provides the guidelines for classifying the information according to its criticality to the institute.
A.7.2.2	Information labelling and handling	An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.	All the assets and data should be clearly labelled and tagged and the documented according to their classification level.
A.8			
A.8.1	**Prior to employment**	**To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.**	
A.8.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with	Roles and responsibilities of users, employees and contractors should be clearly defined according to ISMS

		the organization's information security policy.	
A.8.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	Background verification checks on all candidates for employment, contractors, and third party users should be carried out.
A.8.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.	Terms and Conditions of employment are covered with appointment/contract offer letter for acceptance from prospective employee, it also covers the legal, information security and confidentiality aspects as required in IS Policies.
A.8.2	**During Employment**	**To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.**	

A.8.2.1	Management Responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	Management commitment towards information security is required
A.8.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third-party users, shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	Planned awareness and training sessions shall be organized to provide users and employees trainings on different information security topics
A.8.2.3	Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.	Relevant procedures for disciplinary actions of the isntitute are followed
A.8.3	**Termination or change of employment**	**To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.**	
A.8.3.1	Termination responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	Relevant procedures for termination of employee in the institute should be followed
A.8.3.2	Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their	All personnel are required to return their assets to respective departments who are also notified by HR

		employment, contract or agreement.	
A.8.3.3	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	On instruction from HR, revoke physical or logical access rights
A.9	**Physical and environmental security**		
A.9.1	**Secure areas**	**To prevent unauthorized physical access, damage and interference to the organization's premises and information.**	
A.9.1.1	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.	
A.9.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Logs of visitors should be maintained
A.9.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied	Biometric facility shall be placed in server room

A.9.1.4	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.	Within the organizational premises man-made disasters must be avoided by guarding the physical perimeters or biometric, but Environmental hazard should be covered by installing smoke detectors, fire extinguishers and Emergency Alarms.
A.9.1.5	Working in secure areas	Physical protection and guidelines for working in secure areas shall be designed and applied.	Critical areas are restricted to all but authorized personnel and personnel are only provided access and information in relation to their job roles and responsibilities.
A.9.1.6	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Public Access delivery and loading areas should be separated from operational areas, public areas are monitored by Physical Security Personnel on 24/7 basis through regular shifts.
A.9.2	**Equipment security**	**To prevent loss, damage, theft or compromise of assets and interruption to organization's activities.**	
A.9.2.1	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Servers and critical networking equipment is placed in a restricted access area which is monitored and logged separately.

A.9.2.2	Supporting utilities	UPS and generator systems are in place to ensure continuous power supply to information processing facilities.	Air Conditioners, UPS and generator system must be in place to ensure continuous power supply to information processing facilities. These supporting utilities should be under periodic monitoring and undergo regular maintenance to ensure availability of their services.
A.9.2.3	Cabling security	Power and communication cables should be laid separately and protected from damage or interception by applying appropriate measures. Network cables should be tagged and kept out of paths for quick traceability and avoidance of any incident that could disturb network services.	Power and communication cables should be laid down separately and protected from damage or interception by applying appropriate measures. Network cables should be tagged and kept out of paths for quick traceability and avoidance of any incidents that could disturb network services.
A.9.2.4	Equipment maintenance	Equipment shall be correctly maintained to enable its continued availability and integrity.	Equipment maintenance should be performed periodically to avoid instances that could lead to disruption of services required for business and information security requirements.

A.9.2.5	Security of equipment off premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.	Users shall be provided with guidelines for security of mobile computing devices in their ownership. Security of networking equipment placed off premises should be covered in service level agreements with the concerned organization.
A.9.2.6	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	Procedures for secure disposal of media should be developed and documented. Shredder (physical and logical) should be used to dispose of any media.
A.9.2.7	Removal of property	Equipment, information or software shall not be taken off-site without prior authorization.	Any equipment needed to take off premises should be approved by the owner.
A.10	**Communications and operations management**		
A.10.1	**Operational procedures and responsibilities**	**To ensure the correct and secure operation of information processing facilities.**	
A.10.1.1	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.	Procedures should be documented and maintained by the respective teams in the form of internal SOPs, whereas IS procedures should also be developed to ensure that all operations are performed in compliance with ISMS requirements and information

			processing facilities are utilized under the acceptable guidelines.
A.10.1.2	Change management	Changes to information processing facilities and systems shall be controlled.	All the changes that could affect ISMS should be handled according to Change Management Policy & Procedure
A.10.1.3	Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Job Descriptions should be clearly documented to avoid conflicts in assignments and duties that could create events or incidents effecting Information Security and Business requirements' compliances.
A.10.1.4	Separation of development, test and operational facilities	Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.	Test and production environment should be separated.
A.10.3	**System planning and acceptance**	**To minimize the risk of systems failure.**	
A.10.3.1	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	Capacity assessment should be performed on the basis of previous record of utilization of assets

A.10.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the systems) carried out during development and prior to acceptance.	Criteria for system acceptance should be defined in referenced procedure. In general, any system that creates conflicts with existing management IT should be avoided/removed.
A.10.4	**Protection against malicious and mobile code**	**To protect the integrity of software and information.**	
A.10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	The systems and network are secured against viruses, worms and malicious codes through use of appropriate technologies, solutions and restrictions.
A.10.4.2	Controls against mobile code	Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.	Java applets should be used in Web based application and these applets should be controlled by the application Server
A.10.5	**Back-up**	**To maintain the integrity and availability of information and information processing facilities.**	
A.10.5.1	Information back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	Backup of information should be planned , taken and tested in accordance with the information backup policy and procedure

A.10.6	**Network security management**	**To ensure the protection of information in networks and the protection of the supporting infrastructure.**	
A.10.6.1	Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	Network controls used to manage the network services should be appropriate and parallel to the requirements of both operations and information security
A.10.6.2	Security of network services	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	Technological and application solutions have been adopted to ensure a secure and reliable network.
A.10.7	**Media Handling**	**To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.**	
A.10.7.1	Management of removable media	There shall be procedures in place for the management of removable media.	Access to removable media should be restricted to selective personnel in MIS Cell and head of this department should be responsible for the security of removable media.
A.10.7.2	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.	A documented media disposal policy and procedure should be developed which ensures thorough inspection and cleaning before it is forwarded for disposal and the techniques to

			dispose physical and logical media.
A.10.7.3	Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.	Information handling procedures should be defined in related policies and procedures to ensure protection of information based on its level of classification
A.10.7.4	Security of system documentation	System documentation shall be protected against unauthorized access.	System documentations including policies and procedures should be kept in centralized location in non-editable form for easier accessibility of employees. Actual documentation in editable form must be under the custody of ISMS steering committee who will be responsible to manage its changes and availability of latest version on the network.
A.10.8	**Exchange of information**	**To maintain the security of information and software exchanged within an organization and with any external entity**	
A.10.8.1	Information exchange policies and procedures	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.	Policy need to be developed for protecting the exchange of information.
A.10.8.2	Exchange agreements	Agreements shall be established for the exchange of information	

		and software between the organization and external parties.	
A.10.8.3	Physical media in transit	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	Media containing information should be encrypted and required proper approval before taking out of the premises.
A.10.8.4	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Email Service is available to all users and guidelines shall be provided while developing the email policy
A.10.8.5	Business information systems	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of information systems. Personnel cannot access information that they are not authorized to view or does not belong to their sections.
A.10.9	**Electronic commerce services**	**To ensure the security of electronic commerce services, and their secure use.**	
A.10.9.3	Publicly available information	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.	The integrity of information being made available on a publicly available system such as websites (www.mcs.nust.edu.pk) should be protected to prevent unauthorized modification. And

			the information involved in electronic messaging should be appropriately protected.
A.10.10	**Monitoring**	**To detect unauthorized information processing activities.**	
A.10.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	In order to monitor, review or protect logs, OSSIM can be deployed which can provide security information and event management (SIEM) solution.
A.10.10.2	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	Internal applications being used should records all types of logs and also provides alerts about misuse and failure/denial of access. Moreover administrator activities should also be monitored and recorded.
A.10.10.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Logs and logging utilities should be protected from unauthorized access and also backed up on regular basis along with data and information backup
A.10.10.4	Administrator and operator logs	System administrator and system operator activities shall be logged.	Administrator activities should be monitored and recorded.
A.10.10.5	Fault logging	Faults shall be logged, analyzed, and appropriate action taken.	The log management utilities being used should have the capability to filter out faults.

A.10.10.6	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	All the system clocks should be synchronized with domain server
A.11	**Access Control**		
A.11.1	**Business requirement for access control**	**To control access to information.**	
A.11.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.	An access control policy should be documented and implemented to ensure granting and revoking of access as per job requirement. The policy should cover both logical and physical access.
A.11.2	**User access management**	**To ensure authorized user access and to prevent unauthorized access to information systems.**	
A.11.2.1	User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	New user are registered by the IT department after notification from the HR. In case of termination, HR should notify the concerned personnel to de-activate his/her account.
A.11.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.	Departmental heads will determine what privileges to be given to a team member based on his/her job role. Any privileges given for temporary basis shall be revoked after the requirement is fulfilled.

A.11.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	Users must be provided with a default password and required to change their password on first login according to standard password pattern.
A.11.2.4	Review of user access rights	Management shall review users' access rights at regular intervals using a formal process.	Departmental heads shall be responsible for the review of user access rights according to the job requirement.
A.11.3	**User Responsibilities**	**To prevent unauthorized user access, and compromise or theft of information and information processing facilities.**	
A.11.3.1	Password Use	Users shall be required to follow good security practices in the selection and use of passwords.	Although management enforce changing default and other password after certain period of time but still there is a need to make password management policy in documented form and communicated within the organization to guide users in setting up secure passwords for the applications
A.11.3.2	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Users are made aware not to leave their equipment unattended. Further protection techniques need to be communicated to the users like activating password protected screensavers after certain period of inactivity.

A.11.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	A clear desk and clear screen policy should be documented and implemented to ensure the security of Information available under the custody of users.
A.11.4	**Network access control**	**To prevent unauthorized access to networked services.**	
A.11.4.1	Policy on use of network services	Users shall only be provided with access to the services that they have been specifically authorized to use.	Policy has need to be defined in which responsible administrators have to follow to ensure compliance with IS requirements.
A.11.4.2	User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.	Secure VPN connections must be established for external connections
A.11.4.3	Equipment identification in networks	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.	There should be a policy to identify equipment which authenticate the university's connection from specific locations.
A.11.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports shall be controlled.	Ports should be protected through logical and physical access control under the monitoring and control of IT Operations.
A.11.4.5	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	VLAN are configured for the segregation of network

A.11.4.6	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).	The capability of users to connect to the network should be restricted
A.11.4.7	Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	Network routing controls should be implemented to ensure that the information flow does not violate Information Security of the organization
A.11.5	**Operating System Access Control**	**To prevent unauthorized access to operating systems.**	
A.11.5.1	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.	Secure log-on procedure are in place to access operating systems.
A.11.5.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	Users should be identified and authenticated by domain controllers. However each user has unique user IDs and passwords to login.
A.11.5.3	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.	Systems should be configured to check the validity and expiry of passwords as per defined in password management policy.

A.11.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	
A.11.5.5	Session time-out	Inactive sessions shall be shut down after a defined period of inactivity.	Systems should be configured to automatically log-off from a session in case of inactive response from user end.
A.11.5.6	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.	Limitation of connection time should be configured according to operational requirements
A.11.6	**Application and Information Access Control**	**To prevent unauthorized access to information held in application systems.**	
A.11.6.1	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	System and Network administrators should be responsible to control user access to information as per their privilege level. Users can only access and modify information that they are authorized to use.
A.11.6.2	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.	Sensitive Computing facilities of Exploration Department are isolated from general computing environment
A.11.7	**Mobile Computing and Teleworking**	**To ensure information security when using mobile computing and teleworking facilities.**	

A.11.7.1	Mobile computing and communications	A formal policy shall be in place, and security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	Users provided with laptops are bound to follow Mobile Computing Policy and also have to agree with terms and conditions of laptop usage before the laptop is issued to them. Personal laptops should not be allowed to use for office work.
A.12	**Information systems acquisition, development and maintenance**		
A.12.1	**Security Requirements of Information Systems**	**To ensure that security is an integral part of information systems.**	
A.12.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.	Institutes should do analysis for specifications of purchases in comparison with information security requirements to identify any vulnerabilities and limitation of assets that could be deemed controversial for information security requirements.
A.12.2	**Correct Processing in Applications**	**To prevent errors, loss, unauthorized modification or misuse of information in application.**	
A.12.2.1	Input data validation	Data input to applications shall be validated to ensure that this data is correct and appropriate.	There should be mechanisms to ensure that data input to applications are correct and appropriate, to ensure the integrity of information and output should also be validated.
A.12.2.2	Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	

A.12.2.3	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.	
A.12.2.4	Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	
A.12.3	**Cryptographic Controls**	**To protect the confidentiality, authenticity or integrity of information by cryptographic means.**	
A.12.3.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Deploy PKI Infrastructure
A.12.3.2	Key management	Key management shall be in place to support the organization's use of cryptographic techniques	
A.12.4	**Security of System Files**	**To ensure the security of system files**	
A.12.4.1	Control of operational software	There shall be procedures in place to control the installation of software on operational systems	Operational software should be controlled and managed under the authority of Administrators who ensure that all applications including the OS are updated and their vulnerabilities are controlled through use of

			appropriate measures and tools
A.12.4.2	Protection of system test data	Test data shall be selected carefully, and protected and controlled.	Test data shall be selected carefully, and protected and controlled.
A.12.4.3	Access control to program source code	Access to program source code shall be restricted.	Access to program source code shall be restricted.
A.12.5	**Security in Development and Support Processes**	**To maintain the security of application system software and information.**	
A.12.5.1	Change control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.	Changes to operational systems should be controlled and managed by designated authorities with the required expertise.
A.12.5.2	Technical review of applications after operating system changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Applications should be checked in test environment after any change in operating System before they are considered for live operations
A.12.5.3	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.

A.12.5.4	Information leakage	Opportunities for information leakage shall be prevented.	Network services and application usage should be regularly logged and monitored to identify activities that may lead to or support in leakage of information.
A.12.6	**Technical Vulnerability Management**	**To reduce risks resulting from exploitation of published technical vulnerabilities.**	
A.12.6.1	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	Applications and systems in use should be regularly monitored and their performance should be logged to identify any vulnerabilities in the system.
A.13	**Information security incident management**		
A.13.1	**Reporting Information Security Events and Weaknesses**	**To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.**	
A.13.1.1	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Employees of all levels should be provided with basic awareness of information security event reporting and a procedure needs to be developed for their guidance and understanding.

A.13.1.2	Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	Employees should be made aware of the importance of discovering weaknesses in the system and reporting them to appropriate authorities for timely actions against the associated risks.
A.13.2	**Management of information security incidents and improvements**	**To ensure a consistent and effective approach is applied to the management of information security incidents.**	
A.13.2.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Personnel should be appointed to manage and control information security incidents to record the details, collection of evidences and management of corrective & preventive actions against the issue identified
A.13.2.2	Learning from information security incidents	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	Information Security incidents should be logged along with their corrective actions to learn from history and establish preventive measures to address these issues to stop repetition of events.
A.13.2.3	Collection of evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected,	Evidences in a form log, records, documents, etc. in case of information security incidents should be kept for investigation purposes. These evidences should be kept in secure location

		retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	and are only accessible to authorized personnel
A.14	**Business Continuity Management (BCM)**		
A.14.1	**Information security aspects of business continuity management**	**To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.**	
A.14.1.1	Including information security in the BCM process	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	Critical assets should be identified and prioritized based on their importance in business as well as information security, risk assessment is carried against the known threats and system vulnerabilities. Business Continuity plans should be deployed to ensure continuation of services in case of business interruption.
A.14.1.2	Business continuity and risk assessment	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	Risk assessment is carried out to identify threats and vulnerabilities that could cause a situation of business interruption. Measures should be adopted to ensure Risk prevention measures and business continuity plans in case Risk treatment fails.

A.14.1.3	Developing & implementing continuity plans including IS implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	Business Continuity plans should be developed to identify required resources and steps are needed to ensure uninterrupted business activities (including information security activities) in case a risk were to occur.
A.14.1.4	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	A framework of business continuity plans is to be defined that ensures all plans are consistent, consistently address information security requirements, and identified priorities for testing and maintenance.
A.14.1.5	Testing, maintaining & reassessing BC Plans	Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.	Business continuity plans should be periodically tested and plans are reviewed for revision in light of test result.
A.15	**Compliance**		
A.15.1	**Compliance with legal requirements**	**To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.**	
A.15.1.1	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization

		organization.	
A.15.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	Only approved and licensed Software should be acquired through a formal acquisition process and users are not privileged to install disapproved or invalidated applications.
A.15.1.3	Protection of organizational records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	Organization records should be protected through use of appropriate controls (secure physical storage, restricted access, etc.).
A.15.1.4	Data protection and privacy of personal information	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.	Data and Personal information should be protected through use of appropriate controls (secure physical storage, restricted physical and logical access to information and information processing facilities controls, etc.).

A.15.1.5	Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorized purposes.	Users should be provided with limited accessibilities of information processing facilities to prevent their misuse. An acceptable use of assets policy shall be documented and implemented to ensure acceptable usage of assets.
A.15.1.6	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.	Cryptographic techniques should be used in compliance with legal and regulatory requirements.
A.15.2	**Compliance with security policies and standards, and technical compliance**	**To ensure compliance of systems with organizational security policies and standards**	
A.15.2.1	Compliance with security policies and standards	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	ISMS steering committee shall be appointed to support managers in ensuring compliance with security policy through system reviews and audits.
A.15.2.2	Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.	Information systems shall be regularly checked for compliance with security implementation standards.
A.15.3	**Information system audit considerations**	**To maximize the effectiveness of and to minimize interference to/from the information systems audit process.**	

A.15.3.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems shall be planned carefully and agreed to minimize the risk of disruptions to business processes.	For this, Internal auditing should be performed regularly. This will require the hiring of IT Internal auditor.
A.15.3.2	Protection of information systems audit tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	

*http://www.shjry.com/download/ISO27001_2005_CN.pdf"