SECURED HYBRID CLOUD FRAMEWORK FOR HIGHER EDUCATION IN PAKISTAN

Thesis submitted to Superior College Lahore

In partial fulfilment of requirements for the Degree of

Doctor of Philosophy in Computer Science

By

Muhammad Imran Tariq

PHCS-F14-004

Session: Fall 201-2017

Supervisor

Engr. Dr. Shahzadi Tayyaba

Head, Department of Computer Engineering

The University of Lahore

Co-Supervisor

Prof. Dr. Muhammad Usman Hashmi

Head of the Research

The Superior College Lahore

Faculty of Computer Science & Information Technology

The Superior College Lahore

Abstract

Higher Education in developing countries does not seem as a luxury and has been facing economical limitations like budget, computation power, approach to resources, licensed applications and not unified teaching expertise.

Higher Education Institutions (HEIs) are interested to take benefits of Cloud Computing and its capabilities, but unfortunately, a number of institutions are not well aware of the challenges of the Cloud computing even they did not implement internationally recognized Information Security Framework for their organizations. Literature review revealed that there is no particular Information Security framework for HEIs that discusses complete controls and processes particularly for students and academicians. HEIs have different constraints like cost, resources, etc. so all required information of security controls cannot be achieved.

In this study, multi-method research approach has been used which comprises of four phases. In the first phase, a conceptual cloud adoption framework is developed to understand the challenges that affect the adoption of cloud computing. Survey questionnaire was developed and pilot survey was conducted in HEIs to know about the level of satisfaction regarding legacy system, cloud computing and its services as well as expectations of HEIs. The Structured questionnaires tools were used to generate results like SPSS and SmartPLS.

In second phase, existing renowned information security frameworks that are ISO/IEC 27001:2013, NIST SP 800-53 Rev. 3 and Cloud Control Matrix v3.1 were evaluated by using different risk management methodologies to know their control's effectiveness for Cloud Computing. The output statistics after thorough analysis tantamounts that all these frameworks are not completely mitigating risks related to Cloud Computing.

To address information security requirements and constraints of the Higher Education Institutions in Punjab, Pakistan and to develop comprehensive, cost effective and resourceful security framework particularly for HEIs, the researcher developed the Secured Hybrid Cloud Framework for HEIs comprises of twenty four domains including Information Security Controls for each domain in the

third phase. Furthermore, the researcher also used Fuzzy and Multi Criteria Decision Making technique i.e. TOPSIS to evaluate and prioritize the Information Security Controls to cater the budgetary and cost constraints.

In the fourth phase, agent based security framework is developed keeping in view the information security risks assessment methodologies to implement the secure hybrid cloud framework and its information security controls. The concepts of software agent and intelligent agent have been introduced that collect accurate information used in framework so that a decision system may be developed that will facilitate the Higher Education Institutions to take decision against threat agent on the basis of information provided by the security agents.

Keywords: *Cloud Computing, Higher Education Institutions, Information Security Framework, Information Security Controls, Risk Management, Fuzzy logic, Multi Criteria Decision Making, TOPSIS, SPSS, Smart PLS*

Table of Contents

Abstract ii
Table of Contents iv
List of Figures vi
List of Tables viii
Statement of Original Authorship ix
Acknowledgements x
Chapter 1: Introduction 11
1.1 Introduction to the Study 11
1.2 Problem Statement 12
1.3 Research Questions 14
1.4 Aim and Objective of Study 15
1.5 Significance of Study 16
1.6 Structure of the Thesis 17
Chapter 2: Literature Review 19
2.1 Cloud Computing 19
2.2 The State of Cloud Computing in Government 20
2.3 IT Infrastructure Problems in Higher Education 21
2.4 Information Security 22
2.5 Baseline Manuals / Best Practice Frameworks, Ad-Hoc Approach 22
2.6 Information Security Controls 24
2.7 Fuzzy Logic 24
2.8 Multi Criteria Decision Making 26
2.9 Information Security Control Selection Process 26
Chapter 3: Development of Conceptual Cloud Adoption Framework 28
3.1 Theories and Models of the Adoption of IS innovations 28
3.2 Review of Factors Affecting the Adoption of Technology 31
3.3 The Proposed Conceptual Model 33
3.4 Research Model and Hypotheses 34
3.5 Validation of the Proposed Conceptual Model in Fieldwork 38
Chapter 4: Research Methodology 40
4.1 Selection of an Appropriate Research Approach for Cloud Computing Adoption 40
4.2 Research Philosophy for Cloud Computing Adoption 41
4.3 Selected Research Philosophy 41
4.4 Adoption of the Survey Method for Cloud Computing in Higher Education 43

4.5 Adoption of Case Study Method for cloud computing adoption in higher education ...44
4.6 Research Strategy for the Pilot Survey ...44
4.7 Ethical Considerations for Pilot Survey ...46
4.8 Research Paradigm for the Development of Secure Hybird Cloud Computing Framework ...46
4.9 Selectioin of Multi Criteria Decision Making Methodology ...49
Chapter 5: Survey Research Findings of Cloud Adoption Framework 51
5.1 Questioner Development ...51
5.2 Analysis Method ...51
5.3 Preliminary Analysis ...52
5.4 Descriptive Analysis ...52
Chapter 6: Secured Hybrid Cloud Framework for Higher Education in Pakistan 56
6.1 Analysis of the existing Security Standards and Best Practices ...57
6.2 Secured Hybrid Cloud Framework for Higher Education Institutions in Pakistan ...57
6.3 Reliability of the Proposed Framework ...202
6.4 Comparison of the Proposed Framework With other Renewed Information Security Frameworks ...207
6.5 Effectiveness of the Proposed Framework ...213
6.6 Implementation of Secured Hybrid Cloud Framework Through Agent Based Information Security Framework for Hybid Cloud Computing ...222
6.7 Agents Based Information Security Framework ...222
6.8 Information Security Risk Assessment Methods ...232
6.9 Evaluation of Existing ISRA Methods with ABISF ...232
6.10 Evaluation of Agent Based Informatin Security Framework ...236
Chapter 7: Evaluation and Prioritization of Information Security Controls243
7.1 Selection and prioritization of Information Security Controls ...243
7.2 Background Work ...244
7.3 The Proposed Method ...245
7.4 Step by Step calculation ...252
7.5 Fuzzy TOPSIS Results ...253
7.6 Data Analysis ...260
Chapter 8: Conclusion and Future Work 266
8.1 Research Overview ...266
8.2 Research Contribution ...269
8.3 Suggestions for future research ...271
Bibliography 273

List of Figures

Figure 1. Fuzzy Logic System 24
Figure 2. Fuzzy Model 25
Figure 3. Conceptual Model for the Adoption of Cloud Computing at the Higher Education Level 34
Figure 4. Research Model of Cloud Computing Adoption in the Higher Education Institutions 38
Figure 5. Security Factors Influencing Cloud Adoption 53
Figure 6. Technical Factors Influencing Cloud Adoption 54
Figure 7. Organizational Factors Influencing Cloud Adoption 54
Figure 8. Environmental Factors Influencing Cloud Adoption 54
Figure 9. Advantages Factors Influencing Cloud Adoption 55
Figure 10. Aggregated Comparison of Response of Participants Regarding Factors Influencing on Cloud Adoption 55
Figure 11: Problem Space 59
Figure 12. Secure Hybrid Cloud Framework for Higher Education Institutions in the Pakistan 60
Figure 13. Agent Based Information Security Framework 223
Figure 14. Comparison of 4 Stages of ABISF with other Methods 235
Figure 15. Fuzzy Based Information Security Framework (FBISF) 237
Figure 16. Fuzzy Logic Controller using Fuzzy Based Logic Inference System Editor for Cloud System. 238
Figure 17. MATLAB Rule view 239
Figure 18. 3D Graphs of Sample Solution 240
Figure 19. Trapezoidal Fuzzy Number 246
Figure 20. Linguistic Variables of Effectiveness for the Fuzzy Rates of Alternatives 247
Figure 21. Linguistic Variables of Implementation Time for the Fuzzy Rates of Alternatives 247
Figure 22. Linguistic Variables of Mitigation Time for the Fuzzy Rates of Alternatives 247
Figure 23. Linguistic Variables of Maintenance Cost for the Fuzzy Rates of Alternatives 248
Figure 24. Linguistic Variables of Risk for the Fuzzy Rates of Alternatives 248

Figure 25. Linguistic variables of Budgetary Constraints for the Fuzzy Rates of Alternatives 248
Figure 26. Linguistic Variables of ISC Selection for the Fuzzy Rates of Alternatives 249
Figure 27. Analysis of Preference and Effectiveness weights 262
Figure 28. Analysis of Preference and Implementation Time weights 262
Figure 29. Analysis of Preference and Mitigation Time weights 263
Figure 30. Analysis of Preference and Maintenance Time weights 264
Figure 31. Analysis of Preference and Risk criteria weights 264
Figure 32. Analysis of Preference and Budgetary Constraints weights 265

List of Tables

Table 1. Existing studies examining the adoption of IS innovation 31
Table 2. Independent and Dependent Variables 36
Table 3. Research Hypothesis 36
Table 4. Descriptive Analysis on Cloud Adoption Issues 52
Table 5. Existing CSPs Security Certification and Accreditation. 57
Table 6. Security Dimensions Corresponding to Control 203
Table 7. Information Security Frameworks Comparison Criteria 207
Table 8: Comparison of Proposed Information Security Frameworks with Renowned Frameworks 208
Table 9. Mapping of Security Risks and Threats to proposed Information Security Controls 214
Table 10. ISRA Method Evaluation Criteria 232
Table 11. Comparison of Agent Based Information Security Framework (ABISF) with (ISRA) frameworks 233
Table 12. RESULT COMPARISON 240
Table 13. TrFNs against each Linguistic Variables of input criteria 246
Table 14. TrFNs against each Linguistic Variables of output criteria 246
Table 15. Ranked Information Security Controls 253

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature: _____

Date: _____

Acknowledgements

I would like to thanks my supervisor Dr. Tayyaba Shahzadi for helping me throughout thesis writing process. She always given me positive response, useful remarks and always helped me to stay on track. Her supervision made me able to complete this thesis. I am also grateful for the help from my co-supervisor Dr. Muhammad Usman Hashmi, who gave me additional ideas on how to improve this work. He has given me lot of his prestigious time whenever I required his assistance on critical issues. I feel proud to be called student of them.

I would also like to use this opportunity to thank Dr. Muhammad Waseem Ashraf, Assistant Professor, Government College, University, Lahore, for motivation and help me to publish my research papers in International conferences and Journals.

Last but not least, I would like to thank my family, who made my out of the city studies possible. Without their support, I would not be where I am now. I again do not want to miss this opportunity to salute my mother who always given me time to complete my study.

Chapter 1: Introduction

This chapter briefly comprises of the following aspects: comprehensive problem statement of the dissertation, aims and objectives to achieve of the goals of this study, significance of study, research questions and the structure of the dissertation.

1.1 INTRODUCTION TO THE STUDY

Cloud Computing is one of the most important trends and newest areas in the field of information technology in which resources (e.g. CPU and storage) can be leased and released by the customers through the Internet in an on-demand basis. Cloud Computing has various benefits over traditional computing like reduction of cost, scalability, disaster recovery, ease of implementation and so on but information security and risk management is still a great concern [1].

Cloud computing provides a platform to its users to allocate, reallocate dynamically, configure, reconfigure and de-allocate resources according to their desires. Cloud is based on virtual infrastructure that is unseen to the user which makes almost anyone to deploy tools on demand to serve as many users as desired. The Virtualized cloud infrastructure manages abstraction layer that is necessary for applications or services which are not directly related to the underlying physical infrastructure, such as servers, storage or networks. This service enables the organizations to move resources virtualized infrastructure very efficiently.

The Cloud structure is famous due to its services that have drawn extensive attention of the academicians and organizations. The Cloud resources are provided as services over the internet. The Cloud computing is also facing many roadblocks in its deployment and if these roadblocks do not resolve in due course of time then it will become a great challenge due to its fast growth. Security is one of the great concerns for users especially when they transfer confidential and sensitive information to Cloud server. The fact behind about said the concern is that most of the Cloud servers are operated by the commercial providers which are not under the control of the user. Moreover, confidentiality factor is also arisen when user outsources its data in the cloud. Up shot, the cloud users are feeling insecure as compared to other

environments. It is evident that it is not easy to resolve the security, privacy and confidentiality issues.

Cloud computing has already been taking leverages of virtualization for load balancing. Virtualization also provides security tools, for example it allows the monitoring of virtual machines and management of compound clusters but it is also creating security concerns. Various researches and discussions on virtualization security have been made with different point of views but still virtualization security is a big question mark in its performance.

1.2 PROBLEM STATEMENT

Now in days, cloud computing is topic of modern trend. Almost, every institution of Higher Education is interested to take benefits from Cloud Computing and its capabilities, but unfortunately, a number of institutions are not well aware of the exact challenges of the Cloud computing. The adoption of Cloud computing is essentially and urgently required as every scientific study and researches are currently dealing with Cloud Computing technologies.

The Research revealed that security is a great concern in all deployment models of Cloud Computing [2]. The Higher Education institutions mostly deployed their own Private Cloud to cater their needs related to Information Technology, security and privacy reasons. Apart from other constraints which are also barrier in Cloud Computing deployment, there are several security issues like latency, offline data synchronous, physical data protection, jurisdiction and regulations, data privacy and etc. [3].

The Higher Education Institutions in Punjab, Pakistan and Research fraternity have highly foreign qualified faculty. Each research Centre and University works in disparity because there is no mutual platform to share knowledge with one another even do not have basic infrastructure. For imperishable Education and worthwhile research, it is essential for the students, teachers, and researchers to collaborate with one and other in a single digital platform that is central repository. Owing to lack of centralized digital learning and research resources among researchers and academicians, absence of licensed tools, access on online updated digital library become a cause of various challenges that are presently being faced by the industry, students, teachers and researchers especially the students who are getting education

in remote areas. In Higher Education Institutions, Pakistan there are so many Institutions / Colleges and Universities that have budget limitations, and in current financial crises, the cloud computing is the best solution, especially for the colleges and universities where Information Technology courses are being offered and the use of computers is done in an intensive way.

Owing to stated technical and financial constraints, none of the HEI has implemented internationally recognized Information Security Framework for organizations.

There are several IT Governance and Information Security Management (ISM) frameworks with no infrastructure to mitigate cloud security issues particularly for the Higher Education's Hybrid Cloud. International Organization for standardization (ISO) currently has been developing ISO standards that can be used in cloud organizations and its existing information security standard for ISO/IEC 27001:2013 has not complete controls to address the complete issues pertaining to cloud computing [4]. Moreover, the Cloud Security Alliance has recently developed Cloud Control Matrix v.1.4 from different frameworks and standards but defined controls and matrix in this guide are generic in sense and not specific to HEIs [5]. The National Institute of Standards and Technology has recently introduced SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations which have controls for the implementation of Information Security Controls in an IT organization and even this version of NIST has several controls for the implementation of Information Security in Cloud organization but these controls are not sufficient [6]. The Cloud organizations are deploying different Information Security standards like Federal Information Security Management Act (FISMA), ISO 27001:2013, COBIT 5, NIST SP 800-53 Rev. 4, PCI DSS, HIPPA, SOC 1, SOC 2, SAS 70 Type 1 and FIPS 140-2 but all these are about organizations in general sense irrespective of their size, functionality, objective and goals. Furthermore, these have no specifically controls and processes particularly for education.

Each above stated frameworks, guides and standards that have so many controls and in order to implement all of the controls, organization have to bear heavy cost. HEIs have different constraints like cost, resources, etc. and due to which it cannot implement all required information security controls.

For effective Information Security in HEIs, framework controls have to be evaluated to elicit appropriate controls that fulfil HEIs requirements. Existing techniques for the elicitation of required Information Security controls are inadequate [7]. Inadequate selection of required controls may lead towards failure, increase risks and can impact on overall protection of the system [7]. Fuzzy logic techniques have been used in recent research to mitigate the deficiencies in traditional techniques [7] [8] [9] [10] [11] [12] [13] [14].

This dissertation attempts to identify the concerns and challenges for higher education institutions, while deciding about adoption Cloud Computing technology and propose Secured Hybrid Cloud Framework for Higher Education Institutions consisting of effective information security controls after their evaluation through fuzzy set theory and Multi Criteria Decision Making. This dissertation also attempts for the development of Agent based Information Security Framework to implement the Secured Hybrid Cloud Framework effectively for Higher Education Institutions.

1.3 RESEARCH QUESTIONS

1. Which are the cloud computing adoption factors that may affect the Higher Education Institutions in Pakistan?
2. Which are the Information Security factors that may affect the Higher Education Institutions in Pakistan while adopting of cloud computing?
3. Why is cloud computing still not fully adopted in Higher Education Institutions of Pakistan?
4. How shall Higher Education Institutions in Pakistan be able to adopt cloud computing in the near future?
5. Which are issues in the existing best practices for information security?
6. Why are information security best practices insufficient to deploy in Higher Education Institutions of Pakistan?
7. Which is the need to develop Information Security Controls particularly for Higher Education Institutions of Pakistan?

8. How is an information security control assessment methodology based on Fuzzy TOPSIS address the weaknesses of information security control assessment identified during literature review?
9. How much information about security control assessment methodology is developed with Fuzzy TOPSIS enhance information security in Higher Education Institutions?
10. How can Secured Hybrid Cloud Framework be implemented in the Higher Education Institutions of Pakistan.

1.4 AIM AND OBJECTIVE OF STUDY

Security and Integrity of information in the Cloud Computing is still a question mark. For organization like banks, government agencies, datacenters financial institutions the use of cloud may lawfully require protection of sensitive information due to legal or regulatory requirements. These organizations are still facing information security risks because their information is stored processed process in the service provider's site and they have no physical access to it.

The aims and objectives of this study are given below:-

1. Evaluation of literature about cloud adoption issues critically
2. Assess the challenges while adopting cloud computing in Higher Education Institutions.
3. Understand Technical, Organizational, Environmental, Security issues and Benefits regarding cloud computing in Higher Education Institutions.
4. Suggest a road map for Higher Education Institutions of Pakistan to adopt Cloud Computing.
5. Study existing information security frameworks for organizations to dig-out controls and processes about proposed SHCF.
6. Design Secured Hybrid Cloud Framework for Higher Education Institutions of Pakistan.
7. Develop assessment methodology that considers all-inclusive scenarios while evaluating proposed Information Security Controls.

8. Apply fuzzy logic techniques to develop cost and resources effective controls to improve security more in the HEIs.
9. Evaluate and prioritize the Information Security Controls of the Secured Hybrid Cloud Framework for Higher Education Institutions.
10. Develop comprehensive agent based information security framework for the implementation of the SHCF.
11. Highlight the benefits that Higher Education can enjoy after the adoption of cloud services.

1.5 SIGNIFICANCE OF STUDY

The adoption of Cloud Computing in Education and development countries is a real opportunity. The Cloud computing through its development tools, rapid elasticity and scalability provides a solution to Higher Education Institutions (HEIs) to build infrastructure for education at a lower cost and within time limit. Although Cloud computing has gained importance in Pakistan especially in education and industry, but its impact in Pakistan is still unexplored especially in Higher Education Institutions. In this dissertation, impact of Cloud Computing in Higher Education Institutions has been explored. Challenges to students, teachers, academicians and researchers while opting Cloud Computing have been described. Effective model to adopt Cloud Computing successfully in Higher Education Institutions that will counter roadblocks encountered in the implementation of cloud computing has been described. Finally secured Hybrid Cloud framework for Higher Education Institutions has been developed.

Through under proposal framework:-

1. Solutions will be provided to solve current IT utilizations limitations in Pakistan Higher Education Institutions.
2. Cloud adoption gap has been proposed. Students, teachers, academicians and researchers get benefits of Cloud Applications at a central point.
3. Significant cost of IT resources will be reduced.
4. Higher Education Institutions will be able to do secure communication and access Cloud Services efficiently.

1.6 STRUCTURE OF THE THESIS

This dissertation consists of seven chapters. The brief about these chapters is described below.

Chapter 1: Introduction

This chapter describes about the background of the problem, research aims and objectives, significance of this study that will be met through this work.

Chapter 2: Literature Review

In this chapter, the relevant literature is studied and investigated. A critical review about the cloud computing, gaps in the present knowledge is also discussed in detail. The main focus of the this chapter is the factors influencing while adopting of cloud computing, information security frameworks, Higher Education security issues, Cloud Computing in Higher Education, Information Security Controls, Fuzzy Logic, Multi Criteria Decision Making and the selection processes of the Information Security Controls.

Chapter 3: Development of Conceptual Cloud Adoption Framework

After detailed review about the adoption of Cloud Computing in Higher Education Institutions, literature review was presented to develop a conceptual framework that includes TOE and Diffusion of Innovation (DOI) frameworks. These model are considered to be a comprehensive model for the implementation of cloud computing in the Higher Education Institutions.

Chapter 4: Research Methodology

In this chapter, a relevant and complete research methodology has been applied to carry out this research which has been explained in this chapter. Full details about research methodologies that are adopted, discussed about qualitative and quantitate research. Adoption of survey method, case study of Higher Education, the Research Design Process, research paradigm for the development of the framework, and the selection of Multi Criteria Decision Making have been described in detail.

Chapter 5: Survey Research Findings of Cloud Adoption Framework

Once the initial conceptual framework is developed, pilot survey has to be conducted and then it has to be based on pilot survey that was done to collect the feedback of the participants. Statistical tools have been discussed and the analyzed the results.

Chapter 6: Secured Hybrid Cloud Framework for Higher Education in Pakistan

The reader is briefly introduced about the existing information security standards and framework, a detailed investigations with different criteria has been carried out to evaluate the effectiveness of the controls of these standards and frameworks. Furthermore, this chapter presents the solution to the problem statement. The Secured Hybrid Cloud Framework for Higher Education in Pakistan is developed along with Information Security Controls and discusses in detail. The Reliability of the proposed framework also evaluated by classifying the 175 proposed information security controls according to the Principles of information security, compared proposed framework with other frameworks to show that it works better as compared to other frameworks, and finally conducted risk base analysis of the proposed framework to know its effectiveness for Higher Education Institutions. Secondly, this chapter presents Agent based techniques to implement information security framework and discussed.

Chapter 7: Evaluation and Prioritization of Information Security Controls

This chapter briefly presents to the reader about the existing criteria of selection and prioritization of Information Security Controls. Basing on that literature review, criteria for Information Security Controls evaluation and prioritization are prepared. Methods are proposed to evaluate and prioritize the controls and analyse the results.

Chapter 8: Conclusion

The research results / findings presented in the previous chapters have been described in this chapter. The scope of future work is also encapsulated in this chapter.

Chapter 2: Literature Review

This chapter describes three objectives, to inform the basic of cloud computing and the methods used to investigate it; understanding about current models of cloud computing adoption models, and finally identifying gaps in information security knowledge. The purpose of this thesis is to fill the knowledge gap in the present literature. In this chapter of the research on the adoption of cloud computing, information security frameworks, information security controls, fuzzy logic, Multi Criteria Decision Making and information security control selection processes have been submitted in critical review. The published scientific and experimental publications relates to this thesis are reviewed for said topics.

2.1 CLOUD COMPUTING

Cloud Computing is the most preferred technology of this century. After the introduction of Cloud Computing and its challenges, huge amount of organizations moves towards it. The academicians and educationist play a vital role in its development and opt it with its challenges. The Cloud Computing is providing a number of education related services and its Cloud based Educational platform which is being used by scholars, teachers and students. Google Apps Education is Cloud Computing service available free of cost to the academicians. Microsoft Education Cloud provides free education accounts to academicians. It provides messaging, email, calendar, document sharing, free resources, free social network, web hosting and application testing and deployment tools. Amazon Web Service (AWS) Cloud provides free cost educational resources of Cloud Computing. AWS helps the students to build their own cheap and rapid Cloud Infrastructure. Similarly, Salesforce.com Education Cloud Platform provides multiple educational tools for experiments. IBM Cloud Academy provides access to its educational portfolio for Cloud related projects. Researcher may work on IBM latest Cloud Computing.

The details of Cloud Computing Deployment Models, Service Models, and Cloud Benefits in Higher Education are given under the sub heading of 2.1, 2.2 and 2.3 of Chapter 2 of the Supplementary Material.

2.2 THE STATE OF CLOUD COMPUTING IN GOVERNMENT

It advances in cloud computing technologies mean that many people wonder that if Cloud Computing works for businesses why not for the government? Most companies that provide Cloud Computing solutions to industry are also trade same solutions to private sector companies, and it is surely a good idea for governments to take the advantage of Cloud Computing technology in the coming years. However, before continuing with this, must consider the fact that cloud computing is also facing a number of challenges. Realistically, it may reasonably require a period of about a decade or two for the technology to evolve progressively, considering the breadth, scale and diversity of government applications that they require to address with the adoption of these technologies. Fundamental differences in public and private Cloud Computing applications should be redressed before this initiative takes shape.

It has been repeatedly demonstrated that there is no valid approach for all when it comes to government applications on such a large scale. In fact, considering the diversity and the multitude of government functions, a large number of Cloud Computing solutions can be recommended for government applications, each with it's sharing of limits and challenges in terms of applications and performance.

The details of Cloud Computing in other countries is given under the sub heading of 2.4 of Chapter 2 of the supplementary material.

2.2.1 **State of Cloud Computing in Higher Education Institutions of Pakistan**

Higher Education Universities and Colleges are the backbone of the country through its innovation, research and development. Higher Education in developing countries is often been neglected and has been facing economical limitations like budget, computation power, technical manpower for managing data, approached to research resources, licensed applications and not unified teaching expertise. It perceptibly affects the researchers, the teachers and the learners of the developing countries who have limited or not online digital resources [15].

The Higher Education Institutions of Pakistan has around 700 public sector institutions, colleges and universities. Management of data at a central place (Public Cloud) is a challenging task particularly in respect of universities which have several employees and thousands of students.

Cloud Computing due to its low cost and numerous benefits, is an IT solution in Government Education sector which has budgetary constraints especially in developing countries like Pakistan. Cloud Computing allows Higher Education Institutions, Colleges and Universities to collaborate, share knowledge and resources with one another through internet and by using their existing IT characteristics without having the organization to invest separate huge amount [16].

The collaboration among the researchers, industry, academicians have confirmed their role in the revolution of society and economy of country. The cloud technology is basically used through web browser as the ultimate tool to access all kinds of Cloud services available over the internet. In Education, Cloud Computing offers a number of powerful services that make academicians, researchers, students, administration to access offered applications anywhere, hosted tool, file storage, backup and disaster recovery at anytime and anywhere [17].

Henceforth, universities especially in developing countries have adopted Cloud Computing due to many reasons like low cost of hardware and software, its maintenance, rapid scalability, elasticity, 24/7 access to digital contents, back and quick recovery in case of disaster [18]. During literature review, it has been revealed that a number of renowned universities in the world saved millions dollars of its budget by adopting Cloud Computing in their universities [19].

Cloud computing is the real technology that due to its above said advantages forces the universities of developing countries to rethink about its adoption [20]. In 21st century, internet is available everywhere in developing through different sources and due to very low internet charges, Cloud Computing services and resources are easily available, but despite of this, Cloud adoption and implementation ratio in developing countries is slow.

2.3 IT INFRASTRUCTURE PROBLEMS IN HIGHER EDUCATION

The funding of developing countries for Higher Education is not sustainable while the private institutions are increasing their investment in IT to attract their customers. Although the Government intends to optimize its IT infrastructure with minimum cost as the budget cut is the core issue for the Government of developing countries. The existing IT legacy infrastructures also known as “Private-Cloud” requires maintenance cost that many Government institutions cannot afford due to pressure of cut costs and ultimately old inefficient technology becomes a question mark for

Government Universities and Colleges. The Government is requires to upgrade their old systems on war footing basis. Moreover, these legacy systems and consumes technical staff time for its maintenance. As the invention rate of internet applications are technologies are very high, Government Institutions are required more advanced technologies / solutions to keep them update especially the Universities are offering more dynamic research.

2.4 INFORMATION SECURITY

Information security issues in Cloud Computing hold vital importance as the world's economy depends upon the secure flow of information within and outside the organization. Information security and protection of information assets are critical activities for all Higher Education Colleges and Universities. It improves performance and productivity, detect & defence against threat and increase performance of the Educational systems. In Cloud Computing, information security threats always influence corporate processes and operations directly [21]. Therefore, before implementing cloud computing in higher education, information security issues must be addressed.

To handle these challenges, many worldwide Cloud Computing service providers and customers realized the need to establish an environment for information security governance and follow some type of internationally recognized reference framework, guides, international standards and acts. Several frameworks and standards already exist which can be used for governance and can also be tailored to organizational requirements. During literature review, it has been revealed that research in the areas of Cloud Computing frameworks in Higher Education, Education as Service, E-learning through Cloud Computing, information security governance frameworks, risk management, security and privacy in Cloud Computing, are underway.

2.5 BASELINE MANUALS / BEST PRACTICE FRAMEWORKS, AD-HOC APPROACH

There are many standards, guides, frameworks, and best practices to help manage information security in the organizations. These standards, guides, frameworks and best practices are provided by accredited institutions like International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), British Standards Institute (BSI), Cloud Security Alliance, National Standards Institute of South Africa (SANS) and the Information Security Forum

(ISF). Best practices are widely used by industry to present Information Security Controls. According to Saint-Germain (2005) best practices comprising of standards, guides and frameworks always helps organizations to identify and select Information Security Control. These are also considered as the best practices COBIT, ITIL PROTECT, CCM, ISA and OCTAVE. The ISO, collaboration with the IEC, goals to promote global standards and practices for organizations. To address the fast growth of the internet and dependency on new business information, these both institutions have introduced the IEC series ISO / 27000 to provide effective approach to managing security information.

The authors of [22], developed a manual selection procedure to within framework for selection of appropriate Information Security Controls that meet the requirements of data protection legislation, security objectives and privacy of data protection. European countries have enforced very strict data protection laws that regulate the processing of personal information and also restrict controllers to protect and process data in secure fashion. Therefore, every organization in response of controller requests, demands protection of their data and this improves quality of the services and secure business interest as well.

In this context, [22] a model has been developed that selects an Information Security Controls from a reference manual which meets the legal requirements for data protection and confidentiality requirements of the data controller for the safe processing of personal data.

The section of the most effective and appropriate control from the baseline manual, standard, guide and framework is very tricky and challenging work. The baseline manuals or best practices leave this responsibility on the shoulder of the organizations and sometimes provide limited guidance in the determination of best control to provide responsible safety information.

Moreover, ISC identification through reference manuals do not necessarily take into account the specific limits of the organization, such as: costs, size of the organization, budgetary constraints, and resource limits. However, some formal methods have been developed for the selection of only necessary and desired controls and exclusion of the unnecessary ISCs.

2.6 INFORMATION SECURITY CONTROLS

Information Security Controls are based on policies, procedures, ways to solve the problem, processes involved therein, guideline and functions of the software and hardware among others. The Information Security Controls have been developed, carefully selected according to risk / threat implemented, thoroughly monitored, reviewed at regular interval, and enhanced as necessary to achieve business related Information Security objectives, address and mitigate risks, and enhance Information Security.

The existing renewed information security frameworks like COBIT [23] , NIST [6], ISO [24], CSA [25] and FISMA have so many controls that are not easy to implement to every organization and these frameworks do not have particular controls for the education Institutions. Information Security Controls selection from renowned Information Security standards / guides and frameworks for particular education institutions is critical process. Every framework has a numerous controls that is particular for one organization. So, selection of Information Security Controls and then implement in it educational institution is very tricky process.

During literature review, different techniques for the elicitations of Information Security Controls were noticed and their pros and cons were also studied during literature review. These techniques were traditional techniques and do not provide consider various aspects of the selection criteria for information security controls.

2.7 FUZZY LOGIC

Fuzzy logic is a dominant method used to handle inaccurate and inexact data. It describes, develops and implements complex control systems that facilitates the designers to develop such systems with simple and intuitive methods.

Figure 1. Fuzzy Logic System

Fuzzy logic allows us to develop model with less number of inputs or even without data. Fuzzy techniques have many advantages like lesser dependability on previous values as compared to other complex software. Fuzzy Controller classical is one of the applications, different from other classical applications, which have the

characteristics to utilize human decisions as its knowledge. During fuzzification, users may use inaccurate and unclear statements as input, and it after Defuzzification, generates result to take decision. The Figure 2 is presenting fuzzy model comprises of four input modules. As stated earlier, fuzzification is the first stage of the model, it accepts crisp values and convert them to fuzzy values. Fuzzy values are obtained on the knowledge of users, processed by the inference engine, and then transformed into crisp values by Defuzzification.

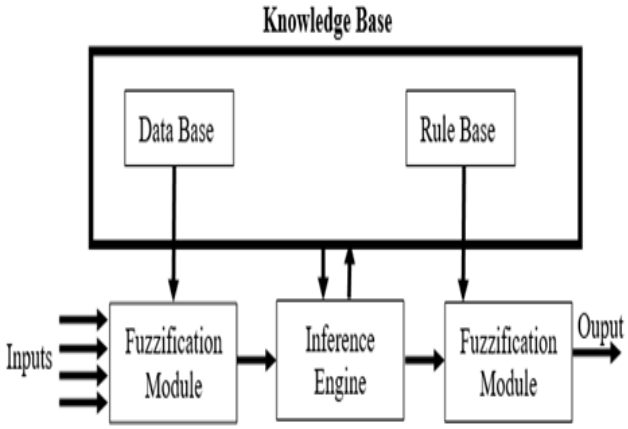


Figure 2. Fuzzy Model

Fuzzy logic has different fuzzy sets and membership functions. Membership functions have values between 0 and 1. At this time, there are eleven membership functions available in MATLAB®. For the evaluation of Agent Based Information Security Framework, only 1 membership function i.e. Triangular was considered.

In 2011, Fuzzy inference has been used for risk assessment using risk matrix [26], whereas in the same year, authors focused on fuzzy logic for risk assessment [27]. The authors applied fuzzy logic for risk assessment and decision making [28]. Similarly, fuzzy logic opted and used by various researchers for risk assessment [27] [29] [30] [31].

Fuzzy logic techniques have been used in recent research papers for cloud computing. A model has been proposed for the evaluation of the user satisfaction about cloud computing and fuzzy logic techniques used for evaluation and to avoid ambiguity [32]. Fuzzy logic techniques were also applied by the [8] to calculate the trust on the cloud service provider which will ultimately increase the reliability of the system. The researcher in its dissertation, investigated various flaws in the traditional Information Security Controls assessment techniques and by using and proposing

fuzzy logic techniques, found relevant Information Security Controls from ISO/IEC 27001:2013 [24]. Risk Management is the integral part of the Information Security and to calculate Risk in the system, the researcher adopted Fuzzy Logic methods to develop Fuzzy Logic calculator for Risk Management [9]. Development of Security strategy in the system plays a vital role in the Information Security System of the organization. The authors at [33], developed fuzzy logic technique to evaluate E-Government Security. The literature review revealed that still there is no relevant criteria developed before to evaluate effectiveness of the Information Security Controls from existing Information Security Controls particularly for Higher Education Institutions using Fuzzy Logic.

Therefore, it is novelty of the research to develop complete information security framework consisting of relevant and particular controls after evaluation through fuzzy logic techniques for Higher Education Institutions of Pakistan.

2.8 MULTI CRITERIA DECISION MAKING

The Multi Criteria Decision Making (MCDM) has proved as an effective methodology to solve a wide variety of multiple classification and ranking related problems. MCDM techniques are useful in many different sectors, like strategic decisions, economic assessment and technology investments. These techniques are also used in the planning, evaluation and selection of information technology (IT). When evaluating decision-making alternatives in new problematic environments, evaluation data for criteria weights and performance evaluations of alternatives in qualitative criteria are often not available and must be assessed subjectively by decision-makers, stakeholders or experts. The subjective evaluation procedure involves two kinds of judgment. Comparative judgments have been used to identify the significance of criteria, while absolute judgments are usually used to evaluate alternatives. On the other hand, both said judgments include fuzziness and partiality, as they involve the thoughts and prejudices of decision makers.

2.9 INFORMATION SECURITY CONTROL SELECTION PROCESS

A formalized control selection process was developed by [34]. The approach involved in the selection and evaluation of ISC includes a process that eliminates the need for random selection; integrated information security policies to formally define the ISC framework including the best ISO / BS 7799. In particular a set of questions

can be designed for high-level companies that analysed the specific business situation and identified the importance of information security. The above has led to the identification of information security requirements proposed by the security policy for private information to be provided in the organization. All security requirements imposed one or more data security policy data that became the part of the organization's public information security policy. Each policy statement was applied within the information security policy written by the ISC framework and one or more ISO / BS best practices said 7799. The authors of [34] have proposed to formalize the CSP approach to business analysis in security requirements and, finally, policies Information security is essential for determining an ISC. However, the process of choosing this ISCs, excluding the need for random selection, still involves a high degree of self-identification in which ISC would ultimately be selected. An ideal case would be if all processes (i.e., from business analysis to ISC selection) could be closely integrated into a formal process subject to a methodology that addresses subjective factors.

Chapter 3: Development of Conceptual Cloud Adoption Framework

In this chapter, empirical studies and the relevant theoretical literature, eventually leading to a conceptual model of the adoption of Cloud Computing by government organizations have been mentioned. The recommended conceptual framework can support the understanding of cloud computing adoption in the Higher Education Institutions. The five parts of this framework are basically based on Technology Organization Environment (TOE) model.

Additionally, the commonly used theories for the adoption of Cloud Computing has been also discussed in this chapter. In addition to understanding the nature of Cloud adoption cases that have been made in the Higher Education Institutions. The proposed conceptual model for the adoption of Cloud Computing could also be used for the adoption of Cloud Computing in other private organizations of Pakistan.

3.1 THEORIES AND MODELS OF THE ADOPTION OF IS INNOVATIONS

The theories about the introduction of new technologies and innovations in information systems were described below after focusing on existing frameworks that discussed about the factors and roadblocks in the adoption process. First time, this type of model was published in the year since 1940. The scholars of social science and industrial studies supported these models. Moreover, the knowledge and diffusion of innovation in the field of Information Security have been based on existing theoretical models for social economics, marketing, budgeting, and psychology [35].

The purpose of adoption of Cloud Computing in private sectors as well as in Public sector gained momentum. Researchers have purposed the frameworks about the factors influencing in the adoption of Cloud Computing in organizations and at individual levels. These studies are based upon empirical analysis. There are many theories that can be employed to see the roadblocks in adoption and still no unified theory exists. These existing theories can be combined to solve different types of problems.

Various researches were conducted to deploy information systems like Technological Acceptance Model (TAM) that is most widely used [36]. Theory of Planned Behaviour is also a technique that can be used for the acceptance of technology in an organization [37]. The TOE framework is the most adopted and efficient type of theory. In this research, TOE and Diffusion of Innovation (DOI) theories were used due to their high applicability.

3.1.1 **Technology-Organisation-Environment (TOE) Framework**

The said framework was initially developed in the year 1990 by Tornatzky and Fleischer. The framework has basically based on three types of components like Technology, Organization and Environment. These are core components that identify the concerns which influence the adoption and implementation issues of new innovation. During literature review, it has been extracted that majority of the studies applied TOE framework to resolve their problems.

The first component / category technological issues involved in the organization such as infrastructure, hardware, software, applications and other technical issues. Whereas, the second category refers to the organizational issues which are related to internal pressure, external pressure, policies of the organization, size of the organization and procedures followed by the organization.

The TOE framework is an efficient and effective framework. It helps the organizations to study the roadblocks in the adoption of new innovations of Information Technology. The wide range of its adoption reveals that it is persistent framework. The TOE framework is applicable to the domain of Information Security. The DOI is also related to TOE framework which emphasized on individual and organizational characteristics consisting of internal and external organizational innovations.

3.1.2 **Theory of the Diffusion of Innovation (DOI)**

The theory of diffusion of innovation was developed in the year 1983 [38]. This study facilities to find out the facilities or hinder in the technology adoption. The main components of this category are advantage, compatibility issues, complexity issues, observability, and trialability [38]. The adoption of new innovation in government sector is very complicated. In order to take final decision, most of the key stakeholders should participate in this process.

3.1.3 **Institutional Theory**

Through Institutional Theory, the events of the organization are explained in different way. The main focus of the Institutional Theory is on the environment of the organization which plays a vital role in the decision of innovation. Efficiency does not depend upon the decisions of the organizations but also depends upon services provided to the society, the legal obligations, cultural factors and the environmental factors in which an organization is working [39].

3.1.4 **Technology Acceptance Model (TAM)**

The Technology Acceptance Model (TAM) was developed by Davis in the year 1989. It recommends an informal link between the variables. Their purposes is to define and assume the factors that influence the behavioural goal of the use of information or computer systems by observing the effects of external factors on behaviours, internal factors and objectives [40].

The TAM is also applied in the field of Information Technology, for example use of word processing, emails and accounting software. Many researchers did their research on Information Technology applied TAM.

3.1.5 **Theory of Planned Behaviour (TPB)**

The TPB is mostly used by the social science students to study the behavioural intension. This is the performance of an entity's reaction against any action. The TPB effectively implemented is the most significant about diverse technologies [41]. It also discusses about the beliefs of an individual. This mostly used to predict the behaviour of individuals against any habit. It is based upon attitude towards the behaviour, subjective norms, and perceived behavioural norms that lead towards intention and then behaviour from intension is got [42]. The TPB is a complete framework that provides systematic investigation about the factors which influence on behavioural choices and efficiently applicable to diverse areas like investment decisions and dishonest actions.

3.1.6 **Integrating DOI, Institutional Theory, and TOE**

It is admitted fact that TOE framework, Institutional Theory and DOI theories give a comprehensive and solid theoretical expansion to the scholars to research technological inventions [43].

Through gone through the existing frameworks, methodologies and techniques, it was concluded that the integration of the DOI, Institutional Theory and TOE were considered the most relevant theories for the adoption of Cloud Computing at public sector.

Moreover, the TOE framework convers the things that DOI theories do not have and their combination make stronger and sustainable framework.

It is practically possible to combine more than one theory to define more categories to cover more issues in the adoption. Therefore, after studying the components / categories of these theories, a list of aspects / factors has been extracted to develop the factors that influence on the adoption of cloud computing.

3.2 REVIEW OF FACTORS AFFECTING THE ADOPTION OF TECHNOLOGY

After studying the above mentioned methodologies, independent and dependent variables were thoroughly studied especially research papers were examined that were relates to study in question. There were many research paper that were discussed these factors and most of the factors that were found in [44] [45]. These factors are given in Table 1.

Table 1. Existing studies examining the adoption of IS innovation

Authors	Methodology	Subject Studied	Variables
Morteza Ghobakhloo, Daniel Arias-Aranda and Jose Benitez Amado [46]	Questionnaire	Electronic Commerce	**Dependent Variable** Post EC adoption **Independent Variable** Perceived relative advantage Perceived compatibility Cost Information intensity CEO s' IS knowledge CEO's innovativeness Business size Competition Buyer/supplier pressure Support from technology vendors
Mumtaz Abdul Hameed Steve Counsell Stephen Swif [47]	Questionnaire	IT innovation	**Dependent Variable** Adoption Decision **Independent Variable** Awareness of innovation Attitude formation of adoption Proposal for adoption Acquisition of innovation User acceptance of innovation Actual use of innovation
Hemlata Gangwar Hema Date R Ramaswamy [48]	Questionnaire	Cloud Computing	**Dependent Variable** Adoption intention **Independent Variable**

Authors	Methodology	Subject Studied	Variables
			Relative advantage Compatibility Complexity Organisational competency Top management support Training and education Competitive pressure Trading partner support Perceived ease of use Perceived usefulness
Yazn Alshamaila and Savvas Papagiannidis [49]	Survey Questionnaire	On-demand computing services	**Dependent Variable** Adoption decision **Independent Variable** Relative advantage Uncertainty Compatibility Complexity Trialability Size Top management support Innovativeness Prior IT experience Competitive pressure Industry Market scope Supplier efforts and external computing support
Jiunn-Woei Liana, David C. Yenb, Yen-Ting Wang [50]	Survey Questionnaire	Cloud Computing	**Dependent Variable** The adoption decision of cloud computing **Independent Variable** CIO innovativeness Perceived technical competence Data security Complexity Compatibility Costs Relative advantage Top manager's support Adequate resource Benefits
Hans P. Borgman, Bouchaib Bahli, Hauke Heier and Fiona Schewski [51]	Questionnaire	Cloud Computing	**Dependent Variable** Cloud Computing Adoption **Independent Variable** Relative advantages Technology complexity Technology compatibility Firm Size Top management support IT expertise of business users Competition intensity Regularity environment Centralized Federal Decentralized Request Prioritize Fund Monitor Enforce Realign
Prashant Guptaa, A. Seetharamana and John Rudolph Raj [52]	Questioner	Cloud Computing	**Dependent Variable** Cloud Computing Adoption **Independent Variable** Cost Reduction Ease of use and convenience Reliability Sharing and collaboration Security and privacy

Authors	Methodology	Subject Studied	Variables
Chinyao Low and Yahsueh Chen [53]	Questioner	Cloud Computing	**Dependent Variable** Cloud Computing Adoption **Independent Variable** Relative advantage Complexity Compatibility Top management support Firm size Technology readiness Competitive pressure Trading partner pressure
Yigitbasioglu, Ogan M [54]	Questioner	Cloud Computing	**Dependent Variable** Intention to increase the level of Cloud Computing Adoption **Independent Variable** Mimetic Pressure Coercive Pressure Normative Pressure Slack Resources TMT Belief TMT Participation
[55]	Questioner	Cloud Computing	**Dependent Variable** Cloud Computing Adoption **Independent Variable** Relative Advantages Complexity Compatibility Top management Support Firm size Technology Readiness Competitive pressure Trading Partner Pressure

3.3 THE PROPOSED CONCEPTUAL MODEL

The TOE structure is a firm theoretical framework that has practical provision and a possible presentation of IS implementation. The TOE structure has environmental factors that DOI theory has not, improved ability to describe the innovation, and business execution. It has been concluded that TOE model is very suitable and complete to the specific needs of the Pakistani Government. As per literature, the organization's IT adoption models, repeatedly studied and observed that it fell within the DOI theory. Therefore, a thorough study of the TOE framework was commenced to understand empirical studies by using only the TOE model, and experimental results link this model with DOI theory, asserts that a similar image in a given theoretical sample can have different factors. Therefore, TOE, DOI and TAM models were used to get improved knowledge to determine the most appropriate cloud adoption factors for the Higher Education Institutions of Pakistan.

This study focuses on the factors that affect the adoption of cloud computing when conducting research at the Educational level. Regulatory obligations and other

barriers were assessed comprehensively evaluated through existing theoretical models that take into account the different aspects of cloud computing.

3.3.1 **An Integrative Conceptual Model**

The proposed model in this dissertation is the combination of three Information Security Models and basically it consists of five themes as shown in the Figure 3. The first theme is above the security factors, second about Environmental and External pressure, third one is about the challenges faced by the Higher Education Institutions, and fourth one is about the Technical factors that are roadblock in the adoption, and the last themes is about the advantages that Cloud users can gain from the adoption of the Cloud Computing.

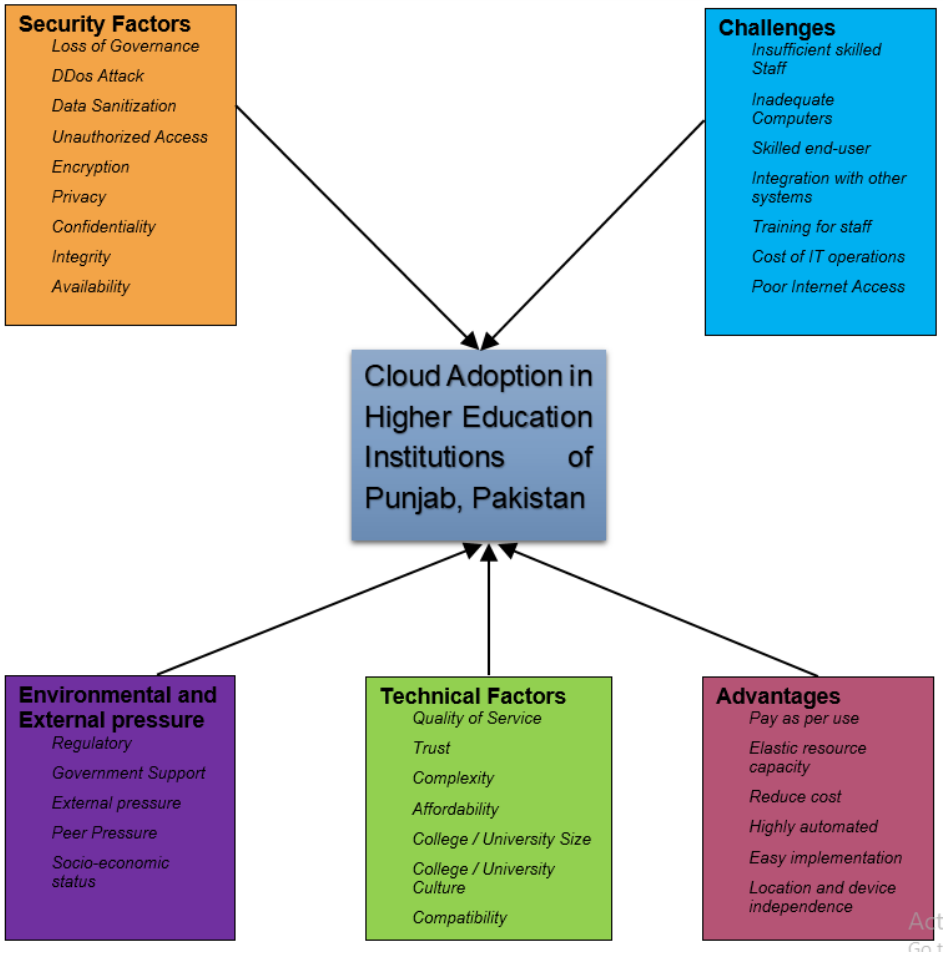


Figure 3. Conceptual Model for the Adoption of Cloud Computing at the Higher Education Level

3.4 RESEARCH MODEL AND HYPOTHESES

In order to in-depth analysis of factors, the model consists of Security, Technical, Organizational Challenges, Environment & External Pressure and Advantages important factors of cloud computing adoption. As Figure 4 shows five contexts

posited 34 predicators for cloud computing adoption in public sector HEIs of Punjab, Pakistan. After in-depth analysis of existing hypotheses during literature review, hypotheses are the particular to the Cloud adoption has been selected and the list of 34 selected independent variables were given in

Table 2, whereas, the research hypotheses are given in Table 3.

Table 2. Independent and Dependent Variables

HN	Independent Variables	Dependent Variable
H1	Loss of Governance	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H2	DDos Attack	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H3	Data sanitization	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H4	Unauthorized Access	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H5	Encryption	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H6	Privacy	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H7	Confidentiality	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H8	Integrity	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H9	Availability	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H10	Quality of Service	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H11	Trust	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H12	Complexity	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H13	Affordability	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H14	College / University Size	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H15	College / University Culture	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H16	Compatibility	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H17	Insufficient skilled Staff	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H18	Inadequate Computers	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H19	Skilled end-user	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H20	Integration with other systems	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H21	Training for staff	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H22	Cost of IT operations	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H23	Poor Internet Access	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H24	Regulatory	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H25	Government Support	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H26	External pressure	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H27	Peer Pressure	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H28	Socio-economic status	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H29	Pay as per use	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H30	Elastic resource capacity	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H31	Reduce cost	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H32	Highly automated	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H33	Easy implementation	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan
H34	Location and device independence	Cloud Adoption in Higher Education Institutions of Punjab, Pakistan

Table 3. Research Hypothesis

HN	Factors	Hypothesis
H1	Security	Loss of Governance has a negative and significant impact on the cloud computing adoption.
H2		Distributed Denial of Service has a negative and significant impact on the adoption.
H3		Data Sanitization have a negative effect on the perceived adoption of cloud computing.
H4		Cloud Computing Unauthorized Access risk is negatively associated with its adoption.

HN	Factors	Hypothesis
H5		Lower degree of encryption in cloud computing adoption has negative impact.
H6		Privacy risks associated with cloud computing adoption has negative impact on its adoption.
H7		Lower degree of Confidentiality in cloud computing adoption has negative impact
H8		Lower degree of Integrity in cloud computing adoption has negative impact
H9		Availability has a negative and significant impact in the cloud computing adoption.
H10	Technical Factors	Perceived benefits of Quality of Service have significant positive effect in the cloud computing adoption.
H11		Trust has significant effect in the cloud computing adoption
H12		Complexity has a negative and significant impact in cloud computing adoption.
H13		Higher degree of affordability in cloud computing adoption has a positive impact.
H14		College / University Size has significant effect in the cloud computing adoption
H15		College / University Culture has significant impact in cloud computing adoption.
H16		Compatibility has a negative and significant impact in cloud computing adoption.
H17	Challenges	Insufficient skilled Staff has a negative and significant impact in cloud computing adoption.
H18		Inadequate Computers has a negative and significant impact in cloud computing adoption.
H19		Skilled end-user has a positive significant impact in cloud computing adoption.
H20		Integration with other systems has significant effect in the cloud computing adoption
H21		Training for staff has significant impact in cloud computing adoption.
H22		Cost of IT operations has a negative and significant impact in cloud computing adoption.
H23		Poor Internet Access has a negative and significant impact in cloud computing adoption.
H24	Environmental and External Pressure	Regulatory has significant impact in cloud computing adoption.
H25		Government Support has a positive significant impact in cloud computing adoption.
H26		External pressure has a positive significant impact in cloud computing adoption.
H27		Peer Pressure has a positive significant impact in cloud computing adoption.
H28		Socio-economic status has a positive significant impact in the cloud computing adoption
H29	Advantages	Perceived benefits of Pay as per use has significant positive effect in the cloud computing adoption
H30		Perceived benefits of Elastic resource capacity has significant positive effect in the cloud computing adoption
H31		Perceived benefits of Reduce cost has significant positive effect in the cloud computing adoption
H32		Perceived benefits of Highly automated has significant positive effect in the cloud computing adoption
H33		Perceived benefits of Easy Implementation has significant positive effect in the cloud computing adoption
H34		Perceived benefits of Location and device independence has significant positive effect in the cloud computing adoption

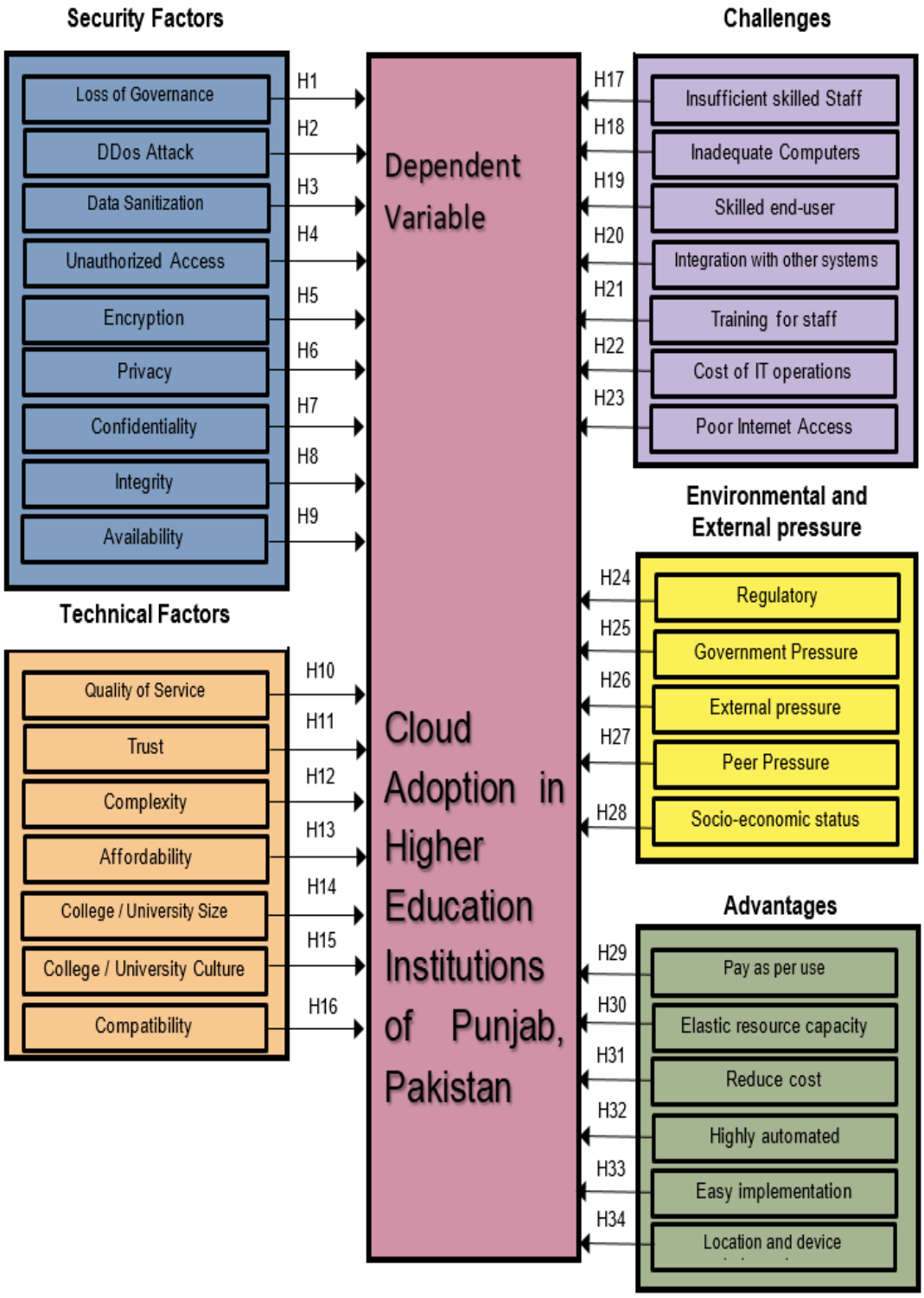


Figure 4. Research Model of Cloud Computing Adoption in the Higher Education Institutions

3.5 VALIDATION OF THE PROPOSED CONCEPTUAL MODEL IN FIELDWORK

The conceptual model proposed in this dissertation is based on different distinct models to formulate an inclusive framework for the learning of the adoption of cloud computing in the Higher Education Institutions of Punjab, Pakistan. So, at this stage

of research, the validity of the proposed framework has been practically tested through different tools like IBM SPSS and Smart PLS for the analysis of the gathered data from the academicians and students.

Chapter 4: Research Methodology

The main goals and objectives of this research have been achieved with the support of research philosophies and methodologies. In this chapter, four distinct methodologies are combined in series. Multimethodology in series is simpler and the most common approach. The massive majority of Multimethodology research involves using diverse methods in series [56]. Therefore, in this thesis, Multimethodology has been used to combine empirical study for the adoption of Cloud Computing in Higher Education Institutions, Design Science Research (DSR) for the development of Secured Hybrid Cloud Framework for Higher Education Institutions includes Information Security Controls, Fuzzy Logic and Multi Criteria Decision Making for the assessment and prioritization of Information Security Controls methodologies within a single intervention. Moreover, highly complex and diverse nature of real-time problems makes Multimethodology involvements a necessary development. By adopting a Multimethodology method, the problem can be handled effectively.

4.1 SELECTION OF AN APPROPRIATE RESEARCH APPROACH FOR CLOUD COMPUTING ADOPTION

The most important aspect of this study is to select suitable research problem. In literature review section, different kind of research approaches have been defined which are necessary to select the correct and specific study. In this modern world, research technologies and methods are expanding day by day, new research approaches have been developed in every discipline. Many research approaches were developed in the field of Information Technology as it is multidisciplinary field [57]. Therefore, there is no single framework which may be considered for the adoption of IT in organization, Information Security Framework consists of Information Security Controls [58]. Different IT adoption related studies was conducted that highlighted different IT adoption issues and redressal techniques [59].

Many questions are asked about the nature of knowledge and how this knowledge has been obtained. The philosophical hypotheses that may be related to the epistemology presented to conduct the research is the ones that has the greatest value [60]. To resolve the problem of this research, the adoption of cloud computing will

be presented for the epistemological position because it is particularly relevant when discussing different types of research philosophies.

4.2 RESEARCH PHILOSOPHY FOR CLOUD COMPUTING ADOPTION

The IS study consists of three main types of models used to conduct empirical studies. First is interpretive school, second critical social school and third is positivist school [57] [60] [61] [62]. Social science models are also multidisciplinary, which explain how it is possible to adopt Information Security models from this fields to study. For knowledge or research, the model can provide a set of common assumptions or ways of thinking [63].

Getting objective and discovering the facts that others revealed, is an important requirement. Positivists believe that this method is the best way to detect and predict a phenomenon. Using the scientific methodologies, objectivity is achieved through the use of statistical methods to test theory and extract results independently, without bias [60]. The key assumption of this kind of method is that there is fact in the world that can be derived using scientific methods. The relationships between variables are measured scientifically and statistically [64], after isolation as independent and independent variables. Using this activity, it is possible to predict the problem to be analysed and explained [65] [64].

Through this research, the idea is to remove any unfair and unjust neutral analysis. There are many conditions in the community that people need to remove, by using this research, it will be possible to extract these conditions [66]. Some ways must be met in this way.

4.3 SELECTED RESEARCH PHILOSOPHY

For this study, the need to select an appropriate methodology, philosophy and research approach is critical because there are many types of information system methodologies and strategies. Cloud computing has been adopted in the public sector as part of this research, which explains why the deepness of the position can be explained, taking into account the view presented by students and academicians as a social aspect of this phenomenon.

Therefore, the researchers opts interpretive method as research methodology. The researcher selected this methodology due to the following reasons:

The phenomenon is interpreted and understood through an explanatory study using the meaning attributed to the students and academicians. The background of the IS can only be understood by understanding the process and impact of the IS and the aspects that influence it [62]. Using this approach, it will be possible to conduct a pilot analysis of factors that encourage or discourage the use of cloud computing in a Higher Education environment. The impact of variables such as Security issues, technical issues, environmental, challenges and administrative factors have been examined to determine the impact of these social disciplines on factors.

Higher Education Institutions have been selected as a unit of analysis. All of which are complex social structures influenced by the awareness of the people concerned. Hence, it is crystal clear that cloud computing is implemented and managed by the people. Therefore, the interpretation approach is considered the most appropriate to use.

Management, regulatory and environmental factors are resolved using the support of cloud computing system. There is no perception of autonomous fact and value, in this case. Since the positive approach emphasizes the existence of separate and independent facts in the knowledge that it has been adopted

In the Higher Education context, the use of cloud computing is a complex phenomenon because it affects and is affected by the phenomenon over time. This technology can be adapted to the current technical or organizational problems as it affects the services provided by organizations to citizens, corporations and other agencies. Therefore, full knowledge of the system is required before it is adopted. The activities being sought should also be analysed, as well as the appointment of effective management staff to operate the system.

The behaviour of stakeholders was taken into consideration when selecting the methodology of interpretation in this report. The adoption of cloud computing at the agency and national levels has been achieved through in-depth understanding and analysis. The Challenges and problems in using cloud computing are one of the main concerns of this research. The use of cloud computing is thus understood by testing a new theory that takes into account the aspects of the school of interpretation and other theories in the literature.

The brief about Qualitative, Quantitative and mixed research methodologies is given under the sub heading of 4.1 and 4.2 of the chapter 4 of Supplementary material.

4.4 ADOPTION OF THE SURVEY METHOD FOR CLOUD COMPUTING IN HIGHER EDUCATION

In applied social research, the survey is a basic measurement method [67]. When quantitative statistics is used in analysis, the survey method is often applied. It is a systematic method that gathers information about a sample of the population. This information provides the rationale for creating quantitative attributes. The population is a large group of people who are contacted; it is possible to collect information about the conduct, or views of these people.

There are 3 different characteristics of the survey. Data analysis can make it possible to discover relationships between variables or to present results to a predetermined set. Survey research is part of a quantitative analysis process that can provide standardized information about the population or sample under study. This sample can be in the form of an organizations, groups, communities, applications, individuals, or projects.

It is appropriate to use the survey in the following cases:

1. When this phenomenon does requires to answers the question "what happens"?
2. When is it not possible to control independent and dependent?
3. The phenomenon of interest should be presented in the natural environment.
4. The phenomena of interest in the recent period or current period must be taken into consideration.

Hypothesis and theories can be evaluated and tested, and the relationships between independent and dependent variables are analyzed by using a survey sample. The in-depth analysis aims at understanding the theoretical expectations of the current variables. The element of cause and effect exists in theory where it is believed that there is a relationship between variables. However, it is also assumed that there is a directional relationship between the variables of an appropriate direction. The existence of cause-and-effect relationships cannot be determined only, but explanatory questions also aim to understand why does this relationship exist? Therefore, the central question for this type of investigation is whether there is a causal relationship to the hypothetical and well-defined reasons?

4.5 ADOPTION OF CASE STUDY METHOD FOR CLOUD COMPUTING ADOPTION IN HIGHER EDUCATION

The case study seems to be the most appropriate way to conduct research on factors that have a direct impact on the adoption of cloud computing by government organizations. This is mainly due to the methodological and philosophical points discussed above. This approach is well suited to the research of information systems and the scope of this research, which depends primarily on organizational factors rather than on technical concerns [57] . This method has been used for many years by many researchers for different subjects [60]. It is widely used by sociologists to explain new situations in daily life. Further details are given under the sub heading of 4.3 of the Chapter 4 of the supplementary material.

4.6 RESEARCH STRATEGY FOR THE PILOT SURVEY

Various research methods have been applied in this study to make it possible to apply the triangulation approach. The multi-method approach has been used to collect data into two main sections. The survey has been used to collect quantitative data; secondly, qualitative data is collected through interviews with security experts and academicians.

4.6.1 **Quantitative Strategy by Using Survey**

The questionnaire-based approach has been used to collect data on the problem of studies. This document has covered the development of the questionnaire, the pilot study, survey protocol and the data analysis procedures.

4.6.2 **Questionnaire Development for Pilot Survey**

The survey method has been used to collect data on factors that may affect the adoption of cloud computing. The literature already exists about Cloud Computing adoption that was used to design the questionnaire. Several similar studies were also used in the literature review to form.

Clear and concise instructions have been provided to the respondents to ensure that the answers are easily readable, clear and in acceptable manner. The nature of the research study for participants was explained. Participants were asked not to write their names in the questionnaires so as not to identify themselves. They were also assured that the information they would provide would remain confidential. The main Higher Education Institutions were students had already been enjoying Cloud

services were selected and copies of the questionnaire were provided to them in person. Several other independent entities also received the questionnaires for participation.

4.6.3 **Survey Pilot Test**

An in-depth investigation plan should include an empirical study. This does not guarantee the full success of the main study, but it gives a certain degree of satisfaction. The pilot study is a feasibility study of the main study. This is a way to test the instruments / techniques / methods before pre-test of specific research that will be used.

The results of the pilot study indicate potential errors or weaknesses in the research methodology or data collection tools. Specific problems can be highlighted and there might be a possibility that the main project would fail. It also indicates what search protocols should be followed; tools should be used and how they will be applied to a successful research project. The authors believes that the pilot test should first and should not be taken into account. The satisfaction of funding agencies is another reason for pilot studies. These organizations need a comprehensive report that shows that the main research project will be successful and that the pilot study can help them address many of the concerns.

The pilot study was conducted in this research after the questionnaire was designed. Five participants used two main objectives. The first objective was to improve the quality of the second questions and to test the respondents' understanding and clarify the survey conducted.

4.6.4 **Survey Protocol**

The questionnaire was prepared and handed over to the students of the Higher Education Institutions of private and public sector colleges. The purpose of the questionnaire was to provide a brief explanation and summary of the importance of research to Higher Education Institutions, without any amount or constraint, or any attempt to influence the results in any way. The questionnaire was designed and distributed in English to 900 students and their responses were received, which served as a base for further analysis.

4.6.5 **Quantitative: Data AnalysisMethods**

There are a number of statistical tools and methodologies that can be used to analyse quantitative data, like tools IBM SPSS, STATA, Smart PL and lisrel. Clear relationships between multiple responses to a questionnaire are often more relevant to the researcher in quantitative analysis than the specific responses themselves.

The Responses to the questions by the participants requiring numerical responses were compiled electronically. The results obtained from the questionnaire have been summarized in Chapter 5.

The survey was conducted on a sample of students, academicians from various private and public Higher Education Institutions of Punjab, Pakistan. Analysis of the data obtained from the survey included two basic processes. The first process involved tabulation of quantitative data by using Microsoft Excel. The second process consisted of encoding quantitative responses, which were statistically analyzed using SPSS. The analysis plan highlighted key research questions, taking into account the elements of the questionnaire, which identified 34 variables as key variables. It was therefore important to tabulate these variables and the adoption of Cloud Computing to determine the response gap. Quantitative analysis of data from descriptive and one-way frequency statistics was extended to inference and regression analyses. Smart PLS is also used to implement different statistical tests. The results have been given in Chapter 5.

4.7 ETHICAL CONSIDERATIONS FOR PILOT SURVEY

During this course of work, efforts were made to respect all ethical considerations in order to protect participants from any adverse impact of the information they provide. The main concerns were deception of privacy, anonymity, accuracy and confidentiality, which was taken into account at all times.

4.8 RESEARCH PARADIGM FOR THE DEVELOPMENT OF SECURE HYBIRD CLOUD COMPUTING FRAMEWORK

The goals of this dissertation are to find out the solution of the Higher Education Institutions when adopting Cloud Computing and implementing Information Security. The solution of this problem was in the form of framework and Information Security Controls. Therefore, it can be claimed that, according to [68], and with the support of [69], the paradigm of design science is very ideal for this thesis. The

design science always create things to solve the human problems. It creates artifacts that resolve organizational problems.

It must be noted that the Design Science Research (DSR) follows a precise research process, in which the key steps lead to the action of a researcher [69]. What distinguishes design science from other standards are the key steps within the research process, namely the design / creation of artifacts and the feasibility assessment. Therefore, the paradigm of design science includes the research carried out by creation or design.

This thesis is based upon the arguments of the researchers noticed during literature review to use the design science as preferred by [68]. The author of [68] combined the opinions of different authors on the paradigm of design science to create a unique definition that eliminates the contradictions among these authors.

In short, the design science paradigm is appropriate and effective to this thesis as a Cloud Computing security issues are being addressed in Higher Education Institutions and a solution has been designed in the shape of framework. To ensure that rigor is maintained in this thesis, a specific and well defined research process is followed, which is described below.

4.8.1 **Research Process**

The authors of [68] developed a methodology and conceptual framework in respect of design science paradigm. There are several researches on design science but all researches are similar. The researcher of this thesis, therefore, used multi approach of design science.

The general steps of the design science research model has usually six steps:

1. Identify problem and motivate
2. Define solution of a solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication

So, in this dissertation, the given above steps are followed for the development of conceptual framework for the adoption of cloud computing, development of

information security framework for hybrid cloud computing and the evaluation of the information security controls:

1. The literature on the Information Security Frameworks in respect of Higher Education Institutions and Organizations was consulted. The objective was to identify and support the existence of a HEIs problem, in particular the inappropriate implementation of information security framework in Higher Education Institutions. Furthermore, there is an attempt to provide substantial support for the importance of solving the Higher Education Institutions problem.
2. The literature was also consulted that provides the solutions of information security framework and Information Security Controls problems relate to Higher Education Institutions. Particular attention was paid to develop Information Security Controls, risk management, introduction of agent based technology, participation of strategic level management in the information security governance.
3. Secured Hybrid Cloud Information Security Framework for Higher Education Institutions in Pakistan was developed and proposed Information Security Controls in HEIs. The proposed framework should be easy to implement and use limited resources of the Institutions.
4. The solution, in the form of Information Security Framework, was implemented in the Higher Education Institutions so that it should be feasible to solve the HEIs problem.
5. The proposed framework was evaluated through Multi Criteria Decision Making and Fuzzy Logic techniques to determine the effectiveness, efficiency and prioritization with which they solved the Information Security problem.
6. The framework and its final findings were incorporated in this dissertation and evidence was provided from three academic peer reviewed journal papers is provided.

To conclude, [68] determined a research process that could be opted within a paradigm of design science. This research process for Secured Hybrid Cloud

Computing framework was used in this thesis, as it has been validated by several authors on the paradigm of design science.

4.8.2 **Research Methods**

It is pertinent to note here that solution to the Higher Education Institution's Information Security problem presented as the goal of this thesis took the form of an artifact, a framework described by modelling techniques. A framework consulted consist of assumptions, methods, way forwards, concepts, techniques, values, and practices that guide to practically solve a problem.

Each research phase in the aforementioned process was addressed using one or more appropriate research methods. The method (s) applicable to each step is presented below:

1. A literature review of Cloud Computing, Information Security Frameworks / standards / guides and Information Security Controls.
2. A literature review of all frameworks development techniques and necessary Information Security Controls for information security governance.
3. Development of framework.
4. Development of Information Security Controls.
5. Select best technique for the evaluation and ranking Information Security controls.
6. To conduct a survey, information security expert belongs to Higher Education invited.
7. Publish the Information Security Framework and Risk Management framework in renowned journals.

4.9 SELECTIOIN OF MULTI CRITERIA DECISION MAKING METHODOLOGY

Many researchers used [70] guideline for the selection of Multi Criteria Decision Making (MCDM) methodology that they used as a solution for the problem under question in this dissertation. After thorough investigation of the existing guidelines about the MCDM and its further types, the researcher of this dissertation selected Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). The details about the selection of TOPSIS was given in Chapter 7 of this dissertation.

Moreover, TOPSIS was a sole combining criteria method. The results of TOPSIS were very easy to understand and explain to the Decision Makers. Further details are given under the sub heading of 4.4 of Chapter 4 of the Supplementary Material.

Chapter 5: Survey Research Findings of Cloud Adoption Framework

A questioner was developed in the light of existing defined adoption contexts and detailed issues were also inserted in security and advantages context to in-depth analysis of the security issues which are more harmful and which advantage are more influential for the students to adopt cloud computing.

The said study was carried out into four stages wherein at the first stage it focuses to find out the exact cloud adoption issues from literature. A theoretical model was developed to construct questionnaire with the consultation of academicians and particularly with the persons related to cloud computing. In the third stage, the survey was conducted by sending questionnaire to the students of the colleges who were studying computer science as subject in the colleges. Finally, different statistical analysis tools were used for descriptive and inferential statistics used to get the output of the questionnaire.

5.1 QUESTIONER DEVELOPMENT

The feedback on the developed questionnaire was recorded in the database to get quantitative data and the in order to test the validity and reliability of the latent variables used in the model. Closed questions (Yes/No) and five points Likert-type scales questions were framed in the questionnaire to get the response of the participants. The questionnaire was developed to cover almost every aspect that can be used in the adoption issues.

5.2 ANALYSIS METHOD

After inserting quantitative data in the statistical analysis tool i.e. IBM SPSS, descriptive results were generated to get statistics about the inserted data. Non-probability convenience sampling technique was used. An Analysis plan was developed based on literature and opinions of the experts. The selected 34 variables were classified Cross-tabulation tests were conducted to get better and different angle results. For Quantitative Analysis, Descriptive, Correlation, Regression Analysis, Factor Analysis, Path Analysis, Reliability and Validity Tests, Independent T-test and One-Way ANOVA were applied.

5.3 PRELIMINARY ANALYSIS

The descriptive statistical analysis of each variable was carried out to measure the responses of the participants in the cloud adoption issues. When the survey was started, more than 1000 participants joined the survey, the questionnaire was checked properly and the survey papers of the participants who did not clear their response, provided incomplete and missing information which was excluded from the array of the survey papers.

5.4 DESCRIPTIVE ANALYSIS

In cloud adoption issues survey, the participant asked Yes / No questions to get their input about which factors they considered are most influential in the adoption of cloud computing and the input of 900 participants regarding cloud adoption issues given in Table 4. The means and Mode of all variable in the descriptive is 1 and the values of SES and SEK are 0.816 and 0.163 respectively for all the variables.

Table 4. Descriptive Analysis on Cloud Adoption Issues

Latent Variable	Mean	SE	SD	SK	KU	Yes	No
Loss of Governance	0.86	0.011	0.34	-2.13	2.55	778	122
DDos Attack	0.85	0.012	0.35	-2.01	2.06	769	131
Data sanitization	0.76	0.014	0.43	-1.23	-0.50	685	215
Unauthorized Access	0.82	0.013	0.39	-1.64	0.69	735	165
Encryption	0.81	0.013	0.39	-1.59	0.54	730	170
Privacy	0.85	0.012	0.36	-1.99	1.96	767	133
Confidentiality	0.87	0.011	0.33	-2.26	3.13	787	113
Integrity	0.81	0.013	0.39	-1.60	0.57	731	169
Availability	0.70	0.015	0.46	-0.86	-1.27	627	273
Quality of Service	0.83	0.012	0.37	-1.78	1.18	749	151
Trust	0.75	0.014	0.43	-1.14	-0.70	673	227
Complexity	0.75	0.014	0.43	-1.18	-0.62	678	222
Affordability	0.80	0.013	0.40	-1.54	0.37	724	176
Size	0.75	0.015	0.44	-1.14	-0.71	672	228
Culture	0.84	0.012	0.36	-1.89	1.58	759	141
Compatibility	0.73	0.015	0.44	-1.05	-0.90	659	241
Insufficient skilled Staff	0.82	0.013	0.39	-1.65	0.72	736	164
Inadequate Computers	0.85	0.012	0.36	-1.98	1.91	766	134
Skilled end-user	0.86	0.012	0.35	-2.03	2.11	770	130
Integration	0.80	0.013	0.40	-1.53	0.34	723	177
Training for staff	0.79	0.014	0.41	-1.45	0.11	714	186
Cost of IT operations	0.83	0.013	0.38	-1.74	1.03	745	155
Poor Internet Access	0.84	0.012	0.36	-1.90	1.63	760	140
Regulatory	0.85	0.012	0.36	-1.99	1.96	767	133
Government Support	0.86	0.011	0.34	-2.13	2.55	778	122
External Pressure	0.88	0.011	0.33	-2.29	3.27	789	111
Peer Pressure	0.84	0.012	0.37	-1.81	1.29	752	148
Socio-economic Status	0.80	0.013	0.40	-1.53	0.34	723	177
Pay as per use	0.84	0.012	0.37	-1.85	1.41	755	145
Elastic resource capacity	0.82	0.013	0.39	-1.65	0.72	736	164

Latent Variable	Mean	SE	SD	SK	KU	Yes	No
Reduce cost	0.81	0.013	0.39	-1.61	0.60	732	168
Highly automated	0.69	0.015	0.46	-0.82	-1.33	620	280
Easy implementation	0.73	0.015	0.45	-1.02	-0.96	654	246
Location and device Independence	0.73	0.015	0.44	-1.06	-0.87	661	239

The descriptive analysis of the data states that 80.44% of the students support cloud computing adoption in the Institutions while 87.66% of students observed External Pressure which is the most important factor in the adoption of cloud computing. Subsequently 87.44% and 86.44% participants agreed upon Confidentiality and Loss of Governance is also the most important factor.

During survey, participant's point of views about the factors influencing cloud adoption are presented in Figure 5 to Figure 10

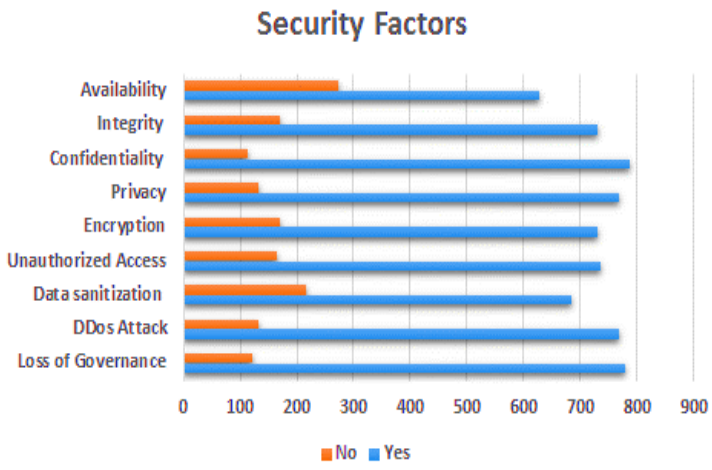


Figure 5. Security Factors Influencing Cloud Adoption

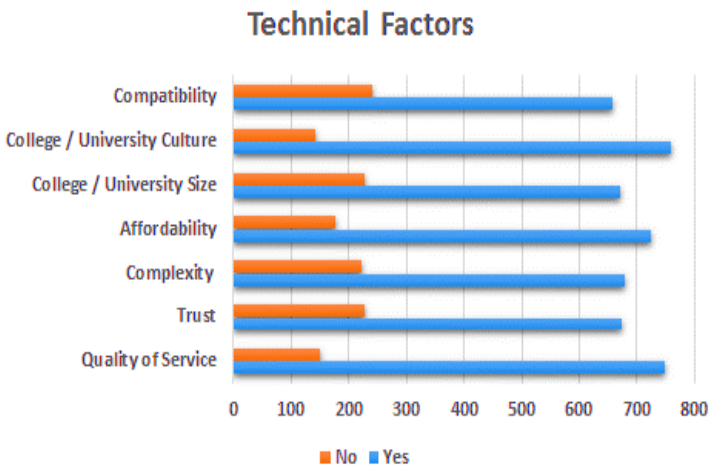


Figure 6. Technical Factors Influencing Cloud Adoption

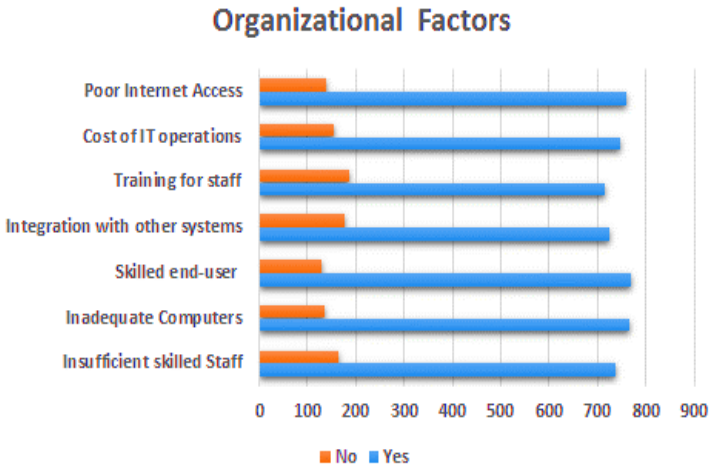


Figure 7. Organizational Factors Influencing Cloud Adoption

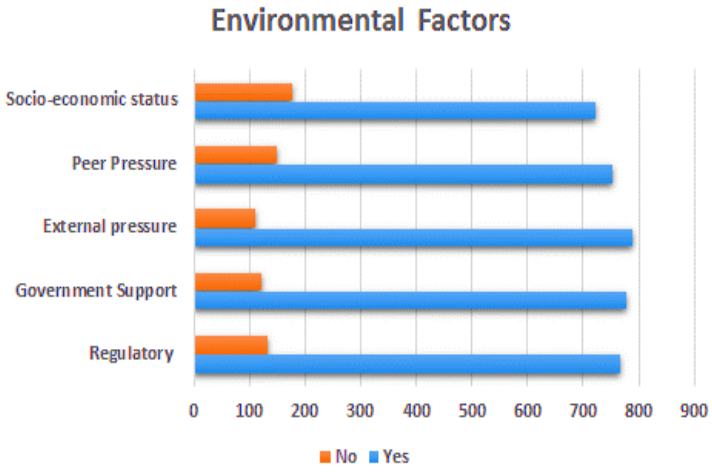


Figure 8. Environmental Factors Influencing Cloud Adoption

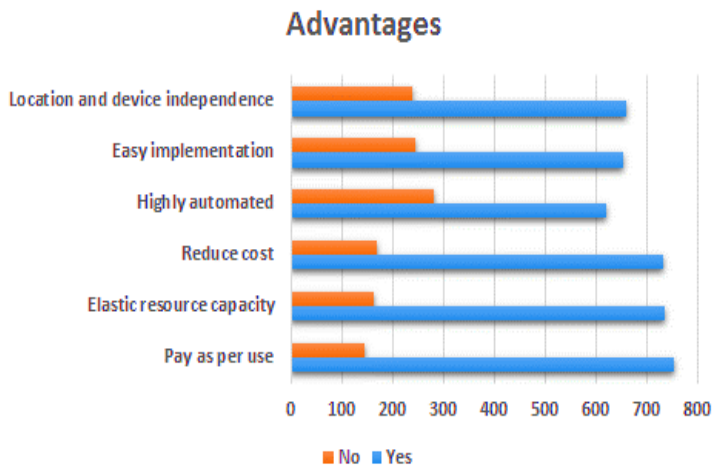


Figure 9. Advantages Factors Influencing Cloud Adoption

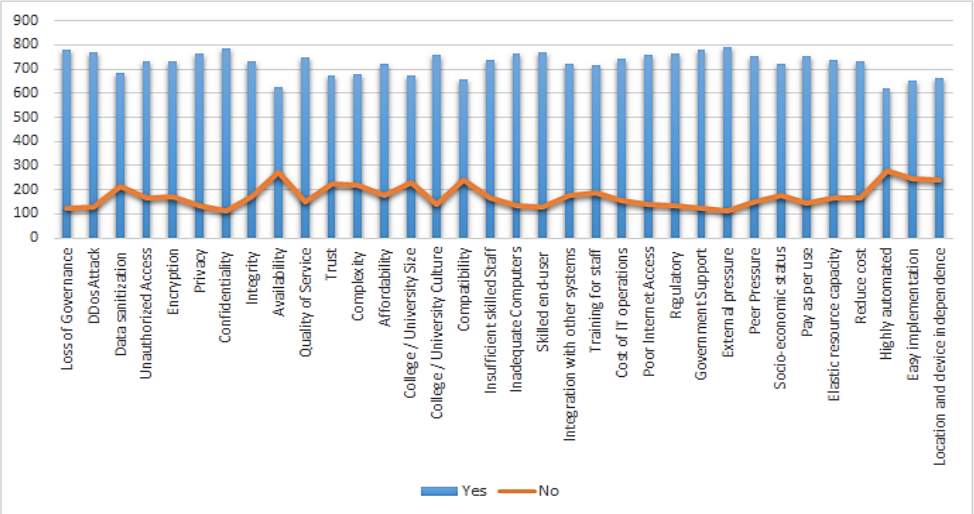


Figure 10. Aggregated Comparison of Response of Participants Regarding Factors Influencing on Cloud Adoption

The reliability and validity test, Inferential Analysis, T-test Analysis, Regression Analysis, Statistical Model, and structural model are discussed in detailed and available in Chapter 5 of the Supplementary material recessively.

The results of the study are very helpful for the Higher Education Institutions of the Punjab, Pakistan by considering influential factors about cloud adoption. This is unique empirical study as according to literature review, such type empirical study has never been done.

Chapter 6: Secured Hybrid Cloud Framework for Higher Education in the Pakistan

Cloud Computing provides a scalable, high availability and low cost services over the Internet. The advent of newer technologies also introduces new risks and threats as well. Although the cloud has a very advanced structure and expansion of services, but security and privacy concerns have been creating obstacles for the enterprise about entirely shifting to the cloud. Therefore, both the service providers and clients should build an information security system and trust relationship with each other. The Survey results discussed in the previous chapter demand secured and comprehensive and also cost effective framework for the Higher Education Institutions. In fact, Higher Education Institutions in the Punjab are running without the adoption of proper and relevant framework. The Higher Education Institutions also have no technical persons to develop security framework and technical expertise to mitigate security risks and threats as well as and removing of vulnerabilities. The current circumstances of the Higher Education Institutions in the Punjab, Pakistan motivated the development of secured hybrid framework.

In this chapter, the most widely used international and industry standard (ISO/IEC 27001:2013), NIST SP 800-53 Rev. 3 as well as Cloud Control Matrix for information security was analysed to know their effectiveness for Cloud Organizations and develop Secured Hybrid Cloud Framework for Higher Education Institutions comprise of Risk Management framework and Information Security Controls. The proposed framework has also been compared with the other renowned information security frameworks. The proposed framework has validated in the light of the information security principles and finally, the author conducted risks based analysis of the proposed framework by identifying cloud based information security risks and threats and mapped these risks to proposed information security controls to demonstrate that the proposed framework and it's IS controls has the capability to mitigate these risks.

6.1 ANALYSIS OF THE EXISTING SECURITY STANDARDS AND BEST PRACTICES

Information security assessment is very good practice to assess the performance of existing information security system and to identify potential risks and exposures

[1]. A security assessment of traditional computing is easy as compliance audit systems are already well established and supported by various existing standards. But [71] said that in the case of Cloud Computing, additional challenges would arise. The Table 5 presents the evaluation of existing security standard certifications that are currently being using by the renowned Cloud Service Providers:

Table 5. Existing CSPs Security Certification and Accreditation.

Organization	Security Compliance
Amazon	SOC 1, SOC 2, SSAE 16, ISAE 3402, FISMA, DIACAP, FedRAMP, PCI DSS Level 1, ISO 27001, FIPS 140-2, HIPPA, CSA and MPAA
Salesforce	ISO 27001, SysTrust, SAS and 70 Type II
Microsoft	FISMA, PCI DSS, HIPAA, SOX, ISO 27001, SAS 70 TYPE 1 and II and NIST SP 800-53
Google	SAS 70 Type II, FISMA, ISO 27001 and NIST SP 800-53
IBM	FISMA, SAS 70 Type II, ISO 27001-2002, SSAE 16, SOC 2, NIST SP 800-53 and HIPPA

There are a number of standards, frameworks and guides that cover the information security area. Cloud organizations can improve their security by implementing ISO / IEC 27001:2013, NIST SP 800-53 Rev.4, FISMA, PCI DSS, HIPPA, SAS 70 and COBIT 5.0. However, these standards are still not covering all the issues and complexities of Cloud Computing. The Risk based analysis of the ISO /IEC 27001:2013, NIST SP 800-53 Rev.3 and Cloud Control Matrix is given under sub heading of 6.1, 6.2 and 6.3 of the Chapter 6 of the Supplementary material.

6.2 SECURED HYBRID CLOUD FRAMEWORK FOR HIGHER EDUCATION INSTITUTIONS IN PAKISTAN

The Information Security Framework (ISF) is a set of rules and procedures that are documented, accepted, understood and processes which define the ways to manage information in an enterprise to reduce risk and vulnerability, and to increase trust in the world that is ever connected [72].

Management challenges in terms of information security are enormous. Even for relatively small organizations, the assets of the information system are important, including databases, files related to employees, company performance, financial matters, etc. [73].

Information Security Management (ISM) is a systematic approach that covers the people, technology, processes and information systems. It also protect critical systems and information by protecting them from risk and threats [74]. Security and confidentiality are among the top ten concerns of management, according to 2017 survey of Cloud Security [75]. The absence of a well-defined information policy is currently considered to be the most serious security problem in organizations [76]. Navigating the myriad of existing security standards, including standards for information security and IT enforcement frameworks, is a challenge for businesses. The framework aims to promote a coherent approach that takes into account an information process view in the context of the organization's operating environment.

The Secured Hybrid Cloud Framework is a complete model that provides complete information security by removing risks relates to Higher Education Institutions. The Secured Hybrid Cloud Framework emphasises not only on technical issues but also on other important elements of the Higher Education Institutions, such as people, processes, Institutional strategies, etc., which also justify the requirement of Information Security. The complete ISF should have following basic elements:

1. Recommended good governance and management practices
2. Recommended Information Security Controls for stakeholders, processes and technology
3. Guide to help harmonize the framework and common and different aspects of commonly adopted standards like COBIT, ISO, NIST, HIPAA, etc.
4. Recommended Risk Analysis and mitigation techniques
5. Manual for implementation and monitoring of Information Security
6. A set of tools that allows organizations to test compliance with the framework

The aim of Secure Hybrid Cloud Framework (SHCF) is to provide a secured Cloud based Educational platform to the academicians, students and teachers of the Higher Education Institutions, Punjab Pakistan. The proposed framework will use exiting traditional IT infrastructure and combine it with Cloud Computing to give secured,

reliable and scalable IT services, solve current IT utilizations limitations, fill cloud adoption gap, reduce significant cost of the IT resources and finally to provide secure communication and access to Cloud Services to Higher Education Institutions (HEIs) of the Punjab so that learning performance and availability of resources may be increased.

Figure 11: Problem Space

The comprehensive Secured Hybrid Cloud Framework consists of three basic components like people, technology, and processes. When these components are properly assembled, the information security program will work together to secure the environment and keep it consistent with HEIs' goal [77] [78].

The Figure 11 shows the problem that the Higher Education Institutions and similar organizations are facing today. The Higher Educations Institutions first of all have no components such as software development, policies, procedures, accident management, business continuity management, organization, auditing, etc. In the case, if any Higher Education Institution has these components then these components are working independently without interacting one another.

The Comprehensive Secured Hybrid Cloud Framework is the solution in which all given above components work together, rather than working in separate orbit. The Secured Hybrid Cloud Framework provides practical guidance for daily IT practices and activities, helping users to create and implement reliable and cost-effective Information Security Controls. Figure 12 shows how the Secured Hybrid Cloud Framework components are interacting with each other to achieve one goal.

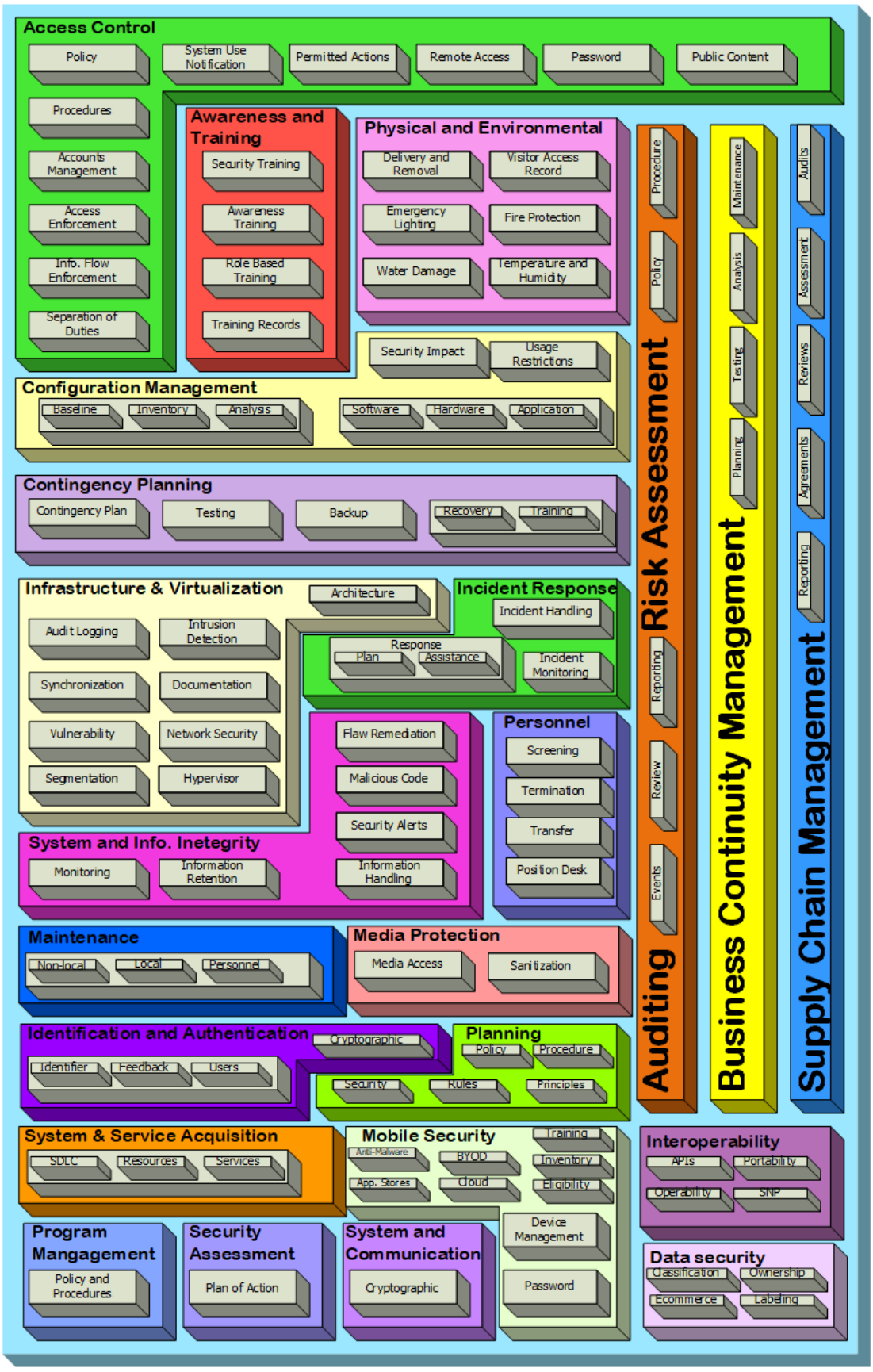


Figure 12. Secure Hybrid Cloud Framework for Higher Education Institutions in the Pakistan

Frameworks are therefore used as models when designing new systems or products. The purpose of the Secured Hybrid Cloud Framework is, therefore, to act as a guide for Higher Education Institutions, that wish to implement and improve the information security system in their Institutions.

After defining the purpose of the Secured Hybrid Cloud Framework and the goals, the principles of Information Security Framework have been used as guidelines for the development of the Secured Hybrid Cloud Framework for Higher Education Institutions. Detailed discussion of the components, relationships and operation of this framework follows the following sub-sections. Furthermore, details about Policies, Procedures and Principles of each domain are given under sub heading 6.4 of the Chapter 6 of the supplementary material.

6.2.1 **Access Control**

The purpose of the Access Control (AC) is to safeguard the Higher Education Institution's information systems. It offers the administrative, physical and technical protections mandatory to manage and control access to information systems in Higher Education Institutions. It defines the requirements of Higher Education Institutions to ensure Access to information assets is legitimate and subject to identification as well as authorization Checks. The purpose of the access control is to ensure that access to all information assets is duly authorized, retained and reviewed. The Access control policy is applicable to all the information assets either physical or non-physical, all users which provides access including physical and local access to HEI's Information System should comply with Access Control. Access to electronic information and information systems housed at the Institute, and the facilities where they are located in Institute premises, is a privilege that can be supervised and cancelled without notice.

Individuals or entities with access to electronic information and information systems at the Institute are responsible for all activities associated with their user credentials. All users are responsible for protecting the confidentiality, integrity and availability of information.

6.5.1.1 Access Controls

Control Number	Control Name	Priority
AC-1	Access Control Policy and Procedures	P1

Statement

Access Control (AC) is basically restriction imposed by the administration to restrict the student and faculty members of the Institution to authorize on resource. Access controls are policies to establish student / faculty member identity, manage user accounts, and monito their access to information resources of the Institution.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

For all Higher Education Institutions who have IT Infrastructure shall develop its own access control policies and regulations. The Higher Education Institution shall document all policies and procedures, disseminate, and review and update after specified interval.

Control Number	Control Name	Priority
AC-2	Account Management	P1

Statement

The University / Institution resources are controlled through logon ID attached with an authorized account. Appropriate management of access controls are essential to make sure the integrity of Institution information and normal operation of Institution management to administrate information resources.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☐ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

1. Before granting authorization access to information resources, formal approval of the Network Administrator is required. The authorization process should be documented and account holders are required to adhere with the terms of use.

2. Each student and incumbent should be assigned unique logon account for accountability purpose. Account must be assigned according to the account policy.

3. During account creation, it is required for the Network Administrator to make sure that only authorized personnel s have granted access.

4. Authorization access has to be changed in accordance with the change in the responsibilities of the incumbent and assignment of the student.

5. Logon IDs that are associated with the students and the employees who are no longer in the Institution are required to be disabled immediately. In case provisional access granted then it must be documented.

6. The Network Administrator must disable logon IDs that have not been used within a reasonable period of time. All such entries are required to be documented.

7. All the students and the employees are required to adhere with password policy and procedure of the administration. Password policy must be enforced while creating account.

Control Number	Control Name	Priority
AC-3	Access Enforcement	P1

Statement

The Institution shall apply approved authorization policy to the system. Management of the Institution should ensure enforcement of the policies to access information technology resources. Access to the Institution's resources are usually controlled through logon ID associated with each legitimate account and proper governance of these access controls is mandatory to make sure the confidentiality and privacy.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

Access control identity, role and rule based policies and its associated concerned enforcement techniques like creation and maintenance of access control lists, develop metrics and cryptography shall be employed by the Institution to control the access between the students/the employees.

Control Number	Control Name	Priority
AC-4	Information Flow Enforcement	P1

Statement

The Information system of Higher Education Institutions must enforce only approved authorizations for the monitoring of the flow of the information within system and between interrelated systems in accordance with applicable Higher Education Institutions policy.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☒ Network ☒ Compute ☐ SaaS ☐ PaaS ☐ IaaS
☐ Storage ☐ Application ☒ Data

Implementation

The Higher Education Institutions must develop information flow control policies, document them and also build enforcement mechanisms to monitor and govern flow of information between specified sources and destinations within Institute information systems and between interconnected systems.

Control Number	Control Name	Priority
AC-5	Separation of Duties	P1

Statement

The Higher Education Institutions shall establish appropriate divisions of responsibilities and separations of duties of individuals as necessary as needed to prevent malevolent activity and eliminate conflicts of interest.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☒ Application ☐ Data

Implementation

The Higher Education Institutions should make sure that proper roaster showing roles and responsibilities of each user has been adequately maintained and placing the same in the information system.

Control Number	Control Name	Priority
AC-6	Least Privilege	P1

Statement

The Higher Education Institutions shall ensure that students, faculty and staff members have only access to those information resources that are required and necessary to accomplish their assigned duties in accordance with Institute mission and function.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Institution should while defining access control procedures given in the AC-2, principle of least privilege must be taken into consideration. Moreover, the Institution shall explicitly define authorizes access per information asset. All privileged roles defined in the system shall be audited to discourage, notice, and report on potential misuse. The configuration of the information systems shall be reviewed and monitored periodically so that non-privileged users can be detected and removed from system.

Control Number	Control Name	Priority
AC-7	Unsuccessful Login Attempts	P2

Statement

The Institution's information management system have to lockout student / employee account after 03 failed login attempts.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☐ Storage ☐ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

Failed logon attempt features must be activated on all the systems of Institution. The Students and the employees of Institution must submit request to reinstate account.

Control Number	Control Name	Priority
AC-8	System Use Notification	P1

Statement

The students and faculty members are required to receive approved notification at the time of login about the system usage, information resources usage procedures, conditions mentioned therein, privacy and security. The notification may retain on the screen till the student or the faculty member log on to access information resources.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

Displays an acceptable to students and faculty member's system use banner before granting them access to IT resources. The login message states that:

1. The students and faculty members are accessing Higher Education Institution system.
2. System usage may be monitored, recorded for audit purpose.
3. Unauthorized use of information system and its resources is prohibited and liable to criminal prosecution.

Control Number	Control Name	Priority
AC-09	Session Lock	P3

Statement

When a student, faculty and staff members uses an IT asset for their assignment, the asset shall automatically be locked whenever asset is found left unattended. The session shall remain locked until student, faculty and staff member provides valid authentication information to again live their session. The session will be automatically lock whenever system or application is left inactive for 30 minutes

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☒ Data

Implementation

The Higher Education Institutions shall be configured to automatically logout the users who are inactive for 30 minutes and to re-gain their session, the users must provide their logon information.

Control Number	Control Name	Priority
AC-10	Permitted Actions without Identification or Authentication	P3

Statement

The Higher Education Institution must identify and document user specific actions that can be performed on the information system without identification or authentication consistent with Institution missions and functions.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Higher Education Institution Systems must identify explicit users. No actions shall be performed on assets till the identification or authentication. Exception may be made in the case of Wireless guest access.

Control Number	Control Name	Priority
AC-11	Remote Access	P1

Statement

The Higher Education Institution is required to establishes, documents and review usage restrictions, and configuration requirements, for each type of remote access allowed. All remote connections are required to fulfil such connections.

1. It is the responsibility of Higher Education Institution student and faculty members to use VPN privileges to access Institution networks with two factor authentication and validated encryption.
2. It is the sole responsibility of all the students and faculty members who are accessing Institution information resources through VPN to make sure that unauthorized users are not allowed to access their institution network.
3. No student and faculty member is allowed to give logon ID and password to anyone even to their close relatives including family members.
4. All the students and faculty members are required to make sure that their system all in and out traffic is crossing through VPN sure tunnel. Moreover, split tunneling is not allowed.
5. All the students and faculty members before connecting their system with Institution Information System through VPN must ensure that their system is protected through up-to-date antivirus software.
6. Pings or other such commends are not to be used to keep the connection open.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

1. All the students and staff members shall take every step to ensure the Confidentiality, Integrity, Availability and Non-Repudiation of information. Moreover, the student and the staff members should understand their responsibilities for the protection of Personnel Identifiable Information (PII) data.
2. All the students and faculty members before granting remote access, must agree to the Institution remote access rules and regulations.
3. In case, the student or faculty member does not use remote access service for 3 months, his / her remote access authorization will be removed and they are required to again contact with concerned person to reinstate their authorization.
4. To get remote access, student and faculty member has to submit remote access grant form to institute for formal approval and institute must verify credential before approval to secure information system.

Control Number	Control Name	Priority
AC-12	Wireless Access	P1

Statement

Wireless Networks are almost used in every institution to cater the network requirements. Higher Education Institutions provide a set of actions that are required to be performed to mitigate security risks associated with wireless technology.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The request for the wireless services of the Institution must be in documents, approved to legitimate students and faculty members, interim guest / visitor's accounts shall be created with specific restrictions on information resources. These

procedures are required to be adhere to maintain integrity, confidentiality and availability of Institute information.

1. All wireless services will be installed on wireless access points and it is necessary to ensure that all wireless security requirements are configured on said wireless access appoints.
2. Unauthorized access points and networks devices must be discouraged to connect with institute network. To accomplish this, continuous / periodic monitoring will be conducted to highlight unauthorized networks and such rogue access points shall be disconnected from the network. Furthermore, security incident will be reported to Network Administrator.
3. The departments of institution are restricted to extend their wireless network without formal approval of the concerned incharge.
4. Only approved students, faculty members and visitors are allowed to access the Institute wireless network.
5. Installation of all types of unapproved wireless equipment in strictly prohibited within boundary of Institute.
6. All Access Points must be protected with strong password, encrypted and only could be accessed through proper authentication mechanism.
7. All students, faculty members and staff members must access through defined network access methods. Similarly, guest accounts will access wireless network through defined methods.
8. The owner of the information resource, or any officer designed by the owner is required to not to allow access of Confidential and sensitive personnel information through wireless communication.
9. All Information Security Controls must be activated, not to bypass or disabled.
10. The default username and passwords of the wireless devices must be changed periodically. Furthermore, broadcasting of SSID may also be stopped.
11. MAC Address filter and IP address filtering should be used to authenticate user.

12. The research associate working with Institution shall also comply with Institute guest account policies.

13. For limited temporary wireless access requests may be entertained subject to approval of the concerned incharge and such type of requests are required to be documented for monitoring and audit.

Control Number	Control Name	Priority
AC-13	Access Control for Mobile Devices	P1

Statement

When mobile devices / handheld devices are used to connect Institute network, an automated measures should be established to authorized legitimate students, faculty members and staff, document their mobile gadgets, and monitor their devices access to information assets. Sufficient information required to be gathered to analyze activates as required.

The Higher Education Institution shall develop policies and procedures to allow only students, faculty members and staff mobile devices. The policies shall clearly identify and document approved and disapproved mobiles to connect with information assets.

Furthermore, Higher Education Institution shall establish usage restrictions, configurations and connections requirements for mobile devices operates within Institution, whether these mobile devices are owned by the organization or the students or the faculty members or even staff members.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

Connection of the students, faculty members and staff members' mobile devices to Higher Education Institution secured network shall be validated by the Institution

concerned as well as all mobile devices must be monitored to identify unauthorized connections.

Control Number	Control Name	Priority
AC-14	User of External Information Systems	P1

Statement

External information systems are the systems or its components that are outside the boundary of the Institution and for which the Institution has no direct control or authority over the applications for the assessment of information security control. If the Higher Education Institution has required external Information system, then trust relationships should be established before using it. The Institution must establish terms and conditions to build trust relationships with other organizations owing external information system. The Students, the faculty members and the staff must obtain permission of the Institute before using an external information system.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

All the connections developed between Higher Education Institutions and organizations owing external information system must be approved and documented. All students, faculty member and staff member must send their third-party connection request to concerned person for formal approval.

Control Number	Control Name	Priority
AC-15	Publicly Accessible Content	P3

Statement

The Higher Education Institutions must segregate information into two categories that is public information and non-public information and also make sure that the information available publically does not contain contents of non-public information. Furthermore, the Institution must review each public information periodically to make sure that it has no non-public contents, review proposed information before posting it publically and remove non-public information from Institute information

system. Students, faculty members and staff must obtain authorization before posting Institute information that is publically accessible.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education	☒ ISO	☒ HOI / Custodian	☒ Network Admn
☒ Faculty Member	☒ Student	☒ Staff Member	☐ Third Party / CSP
☐ Assets / Resources	☐ Visitors		

Cloud Architectural Relevance			**Cloud Service Delivery Model**		
☐ Physical	☒ Network	☒ Compute	☒ SaaS	☒ PaaS	☒ IaaS
☐ Storage	☒ Application	☐ Data			

Implementation

1. The Institute must designate and authorize individuals to post information publically.
2. The designated individual must make sure that public information does not contain any non-public information.
3. The designated individual also must review proposed contents of information before available it to publically.
4. Review each public information periodically to make sure that it has not contents of non-public information.

Authority: [79] [80] [81] [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93] [94] [95] [24] [6] [20] [23]

6.2.2 **Awareness and Training**

It defines requirements for information security and cyber security awareness, training and education for faculty members either teaching and non-teaching of the Higher Education Institute who have access to the Institute's information systems, resources and assets in accordance with the said framework. All the users of the Information system shall make sure that their use of the Institute system is effective and does not create threats and risks for information security. The Heads of the Institute shall play lading role by ensuring that information security is top on priority. The Information Security Officer and Head of the Institute shall provide regular, relevant, comprehensive training to all employees through various means like seminars, newsletters, meetings, pamphlets and briefings. The Heads of the Institute

shall receive input from Information Security Officer and all the staff members on the effectiveness of said training and measures to improve it.

6.5.2.1 Awareness and Training Controls

Control Number	Control Name	Priority
AT-1	Security Awareness and Training Policy and Procedures	P1

Statement

The purpose of this control is to develop, document, opt, adhere a formal security awareness and training program that address scope, role, responsibilities, compliance and purpose and coordination between entities.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

All students, staff members, and faculty members who use information resources are required to read and understand all training related procedures and policies and comply with these Compute security policies in true letter and spirit.

Control Number	Control Name	Priority
AT-2	Awareness and Training Controls	P1

Statement

Understanding the importance of information security, individual responsibilities, and accountability are paramount to achieve the Institute security goals. This can be accomplished with a combination of general information, security awareness training, and targeted training. The security awareness and training information needs to be ongoing and updated as needed.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

All Higher Education Institutions personnel who uses systems are required to adhere with the procedures related to this control. For convenience, a method is listed below to use information security awareness training.

1. All new employee of the Higher Education Institution shall get ibid training prior to the use of information resources of the Intuition or at least within 15 days.
2. After completion of training, all faculty and staff members must produce certificate that they have read every clause and its sub clauses thoroughly, understood it and will adhere all security related policies and procedures of the Institution.
3. Refresh courses should be conducted on annual basis and every faculty and staff member of the Institution must participate in it.
4. Higher Education Intuitions may require extra incidental training and need acknowledgement as determined by the Higher Education Intuition.
5. Higher Education Institution IT personnel should workout to introduce new security awareness trainings, communicate new introduced program and generate security bulletin.
6. The Heads of the Institutions should ensure that all faculty members and staff members are properly trained to perform their duties and responsibilities related to information security.

Control Number	Control Name	Priority
AT-3	Role Based Security Training	P1

Statement

All the Higher Education Institutions must provide training related to their roles in addition to their training at the time of their induction and when Heads of the Intuition conduct training on Information System changes.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

All the Heads of the Institutes are responsible to conduct role-based security training in their Institutions for their staff in respect of their security responsibilities.

Control Number	Control Name	Priority
AT-4	Security Training Records	P3

Statement

All the Higher Education Institutions shall properly maintain IS awareness training records.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

All the Heads of the Intuitions shall document all information security training programs, monitor each training activities, evaluate performance of each trainee, maintain individual training records, liaison with Human Resource Department to

update the record of incumbents and take action against the trainees who don't perform their training assignments.

Authority: [79] [80] [81] [82] [83] [84] [93] [94] [95] [24] [6] [20] [23]

6.2.3 **Audit and Accountability**

The goals of this domain is to define audit and accountability requirements that will support in evaluating the adequacy of system controls, confirming compliance with outlined policies and operational measures, and exceptionally finding the actions of system users. Audit and Accountability policies and procedures will assist Higher Education Institutions in maintaining a consistent, effective and reliable record of information system activities. When audit and accountabilities are properly implemented, information system can help in preventive measure as well as a forensic assistance. An inclusive record of "who-did-what-when" can be used to discourage asset abuse or can act as evidence.

The requirements described in this policy will aid to make sure that data owners of the Higher Education Institute and system owners have a clear view of the security situation of information systems. In case of an accident, the audit and accountability measures will provide a checkable record to determine the cause.

6.5.3.1 Audit and Accountability Controls

Control Number	Control Name	Priority
AU-1	Audit & Accountability Controls	P1

Statement

The Higher Education Institutions shall prepare a document for Audit and Accountability regulations to manage identified and prospect risks from event logging and traffic monitoring of each user. The Audit and Accountabilities controls will facilitate Higher Education Institutions to implement best security practices in respect of auditing and accountability.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The owner of the Institute or Network Administrator will develop and maintain policies and procedures comprising of scope of controls, roles and responsibilities of individuals, method of liaison between the concerned personnel, commitment of management and compliance of Higher Education audit and accountability program.

Control Number	Control Name	Priority
AU-2	Audit Events	P1

Statement

All the information resources of the Higher Education Institution must have ability to perform auditing actions against each user transaction to be required to trace.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The owner of the Institute or Network Administrator shall maintain the record of auditing and monitor access to all Institutional IT resources including all network devices, operating systems, applications, databases, all remote access connections and access to accounts. Audit related records should be capacitated to generate information security related events. The owner or Network Administrator shall enable event auditing and monitor each event log carefully to identify and report suspicious activities. The auditable events shall be reviewed every year.

Control Number	Control Name	Priority
AU-3	Content of Audit Records	P1

Statement

The Higher Education Institution must make sure that their information system is properly generating audit record containing information about the occurrence of event, time stamp of event, location of the event, source of the event, output of the event, description of the event, success/failure indicator, associated access controls, associated regulations and procedures and associated information resources with the event.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

All the Higher Education Institutions must make sure that their information security system is configured to provide centralized logging. Automatic logging must be configured against each information resource. The following events must be captured in additional to other events that Institute desire to configure.

1. All logon to system.
2. All logoff to system.
3. Change of accounts password.
4. All commands executed by the system administrator.
5. Changes in security rules of firewall, anti-virus and intrusion detection.
6. Changes to audit and logging settings.
7. Start-up and shutdown of all audit related functions.
8. Clearing of audit log.
9. Privilege escalations.

10. Remote Access and dial-in access to system.

11. System administration.

12. Changes in the critical record of the applications.

Control Number	Control Name	Priority
AU-4	Audit Storage Capacity	P1

Statement

The Higher Education Institutions must allocate sufficient storage capacity for store audit record and this audit record must be able to be retrieved as and when required for action. The storage capacity must be allocated on the number of auditing functions and processing requirements.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information system of the Institution must be configured to maintain and monitor all logs at a centralized log server and this server has sufficient storage capacity to retain all logs.

Control Number	Control Name	Priority
AU-5	Response to Audit Processing Failures	P1

Statement

The Information System of the Higher Education Institutions must be configured in such a matter that if audit processing system fails, then it should generate alert to the designated officials and it also must be configured to take suitable action on account of audit log failure. Furthermore, the system must have auto-correct function to return to normal operations. The owner of the institute or Network Administrator must design a plan to use in audit processing failure.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Systems of the Higher Education Institution shall generate alerts to the Network Administrators in the case audit processing system fails, take action and invoke auto-correct system to return to normal operations.

Control Number	Control Name	Priority
AU-6	Audit Review, Analysis, and Reporting	P1

Statement

The Higher Education Institution system must be capable to generate automated reports and send it to the designated personnel who shall review and analyze reports immediately to identify unfamiliar activity and initiate action if feels necessary. The Head of the Institute or Network Administrator shall document all reports and time frame to review the reports. Furthermore, if there is a change in the risk, assets of the organizations and change in operations, the level of review, monitoring and analysis must be adjusted accordingly.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute or Network Administrator must make sure that system generated mission critical logs are periodically reviewed, automated system is functioning up to the mark and system is generating alert on inappropriate activity. It

is pertinent to add here that for non-mission critical systems, it is required to make sure that logs are reviewed on the basis of risk management decisions.

Control Number	Control Name	Priority
AU-7	Time Stamps	P1

Statement

All Higher Education Institutions are required to use internal information system synchronized clock to generate time stamps (date and time) to use in the captured event. The time stamp must be an inherited property for event logs and it must be synchronized.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Institution information systems should be configured in a manner that for audit record, it is always used an internal system clock to generate time stamps. The internal clock may be synchronized to NTP server if required.

Control Number	Control Name	Priority
AU-8	Protection of Audit Information	P3

Statement

The Higher Education Institutions shall identify responsible, trained information security experts who will responsible for reviewing audit information generated by the system. Furthermore, access rights should only be granted to those authorized personnel to this information. Audit log of the information system must be protected by strong access system to prevent the system from unauthorized access. Upshot, the HEIs system should protect audit information and tools from illegal access, change, and removal.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute or Network Administrator should make sure that all audit logs are adequately protected and only legitimate / authorized / designated users have rights to access information.

Control Number	Control Name	Priority
AU-9	Audit Record Retention	P1

Statement

All the Higher Education Institutions must keep audit records for adequate period of time to provide support during inspection of information system, risk management, threat management, future audit, monitoring of security incidents and to meet regulatory requirements.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute or Network Administrator should retain audit record permanently to provide support in future investigation.

Control Number	Control Name	Priority
AU-10	Audit Generation	P1

Statement

The audit system of the Higher Education Institution should allow investigators to let them select auditable events required to be audited according to their choice, the audit records must also provide to them and auditing tools should also be provided to generate effective report.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network administrator shall comfiture Information System in such a manner that it shall automatically generate audit reports and preserve audit record.

Authority: [79] [80] [81] [82] [83] [84] [86] [93] [92] [94] [97] [95] [24] [6] [20] [23]

6.2.4 Business Continuity Management & Operational Resilience

The business continuity program at Higher Education Institutions is proactive and iterative in its method to evaluate potential risks and ensuring that appropriate and sustainable agreements are implemented. The Program must support the safety of HEIs employees and ensure security of critical resources which are necessary to continue with key business processes and reduce impacts in a cost-effective manner within stipulated time limit in the case of if any interruption occurs.

The main objective of Business Continuity is to allow the Head of the Institute and Information Security Officer to continue to manage and operate has Institute under adverse conditions, taking advantage of adequate resume strategies, recovery objectives and business continuity and crisis management plans. In other words, Business continuity plans are developed to establish appropriate and sustainable operations of business services in the event of disaster or any unpleasant event.

6.5.4.1 Business Continuity Management & Operational Resilience Controls

Control Number	Control Name	Priority
BC-1	Business Continuity Management & Operational Reliance	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of Business Continuity Management & Operational Reliance Policy and Procedures, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of Business Continuity Management & Operational Reliance Policy and Procedures and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the Business Continuity Management & Operational Reliance Policy and Procedures.

Control Number	Control Name	Priority
BC-2	Business Continuity Planning	P1

Statement

The Higher Education shall develop Business Continuity Plan through unified framework. The plan shall address Information Security Requirements, priorities requirement and also test these before implementing.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer shall prepare Business Continuity Plan by defining the exiting deficiencies in the Information Security System, nominate the personnel who shall be responsible to review, update as required and approve it, roles and responsibilities of the concerned personnel, recovery plan and its invocation.

Control Number	Control Name	Priority
BC-3	Business Continuity Testing	P1

Statement

The Higher Education shall before implanting Business Continuity Plan, test all the security incident responses at planned intervals, or as necessary and document all testing results.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer shall prepare incident response plans, test each incident response, and document all incident responses before finalizing Business Continuity Plan. The incident plans shall cover all prospect and potential incidents relates to students, faculty members, staff members, venders, third-parties and supply chain related dependencies.

Control	Control Name	Priority

Number		
BC-4	Datacentre Utilities / Environmental Conditions	P2

Statement

The environmental conditions like humidity level, power supply, water connections, UPS, internet connection should be secured. The said conditions should be monitored, tested at planned interval and document to make sure protection from unauthorized access, interception and damage.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☐ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☐ Data

Implementation

The Head of the Institute and Network Administrator of the Institute shall make sure that all environmental conditions of the Institute and Information Security System are properly tested at regular interval and document each test.

Control Number	Control Name	Priority
BC-5	Equipment Location and Maintenance	P2

Statement

All the assets and equipment of the Information System are required to be kept away from the locations that have environments risks and hazards. The equipment are required to be placed at a place that is at reasonable distance from the Institute. The maintenance of the equipment at the remote site should be continuity maintained and also should make sure that equipment are available to maintain and support staff as and when require.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☐ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☐ Application ☐ Data

Implementation
The Network Administrator is required to place the IT equipment in risk free environment and reasonable distance from the Institute.

Control Number	Control Name	Priority
BC-6	Impact Analysis	P1

Statement
The impact of any disruption and interruption to the organization due to students, faculty and staff member is required to be determined and documented. To calculate disruption and interruption, the critical services, products are require be identified, number and nature of dependencies on applications, venders, partners and third parties, tolerance of the system in case of disruption, priorities and time of recovery, assumption time for critical products and resources required for assumption.

Applicability
This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.
☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**
☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation
The Information Security Officer and Network Administrator is required to calculate interruption and disruption due to any sudden attack or any due to students, faculty and staff members. The Network Administrator should consider the factors of disruption and interruption given in the description of this control.

Control Number	Control Name	Priority
BC-7	Retention Policy	P2

Statement
For continuity of Institutional Information System, policies and procedures are required to be established along-with supporting defined measures to be taken. Retention period of every critical asset of the Information System is required to be

defined as per defined policies and procedures, as well as legal, financial, statutory and regulatory obligations. The most important policy is Backup and Recovery and its measures should be the part of Institutional continuity plan and shall require be tested at regular interval or as necessary.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance			**Cloud Service Delivery Model**		
☒ Physical	☒ Network	☒ Compute	☒ SaaS	☒ PaaS	☒ IaaS
☒ Storage	☒ Application	☒ Data			

Implementation

The Information Security Officer of the Higher Education and Network Administrator of each Institute is required to establish, monitor, update, review and maintain policies and procedures with the support of concreate well defined measures.

Authority: [93] [94] [95] [24] [6] [20] [23] [98] [99] [100] [101] [102] [103]

6.2.5 Configuration Management

Information systems are mostly dynamic, changing the system state frequently due to hardware, software updates, or environment modifications in which system is operating. Every Industry standard emphasizes that changes in information systems should be documented and evaluated the potential impact of proposed changes to the system in operational and security situations. IT industry best practices recognize this as a key aspect of effective system management, as well as being part of ongoing monitoring and maintenance of security accreditation. Configuration management is an important control to ensure the safety, security and reliability of HEIs information systems. If there is no control process to handle configuration changes, the administration cannot ensure that its systems work as expected, or that system maintenance will be done in a cost-effective or timely manner.

This module provides the configuration management requirements required to ensure that information systems are designed and configured with sufficient controls to protect the Higher Education Institute information systems. If the Institute

infrastructure are not protected from threats and risks then institute may lose data integrity, data unavailability, or unauthorized use of data or information systems that are Institute devices have.

The purpose of this module is to establish Configuration Management Program throughout the Institute and to provide tasks and compliance requirements and the general principles of Configuration Management processes. The outlined policy is applicable to all the Institute's hardware, software, applications and documents that can impact on the performance of the Institute.

6.5.5.1 Configuration Management Controls

Control Number	Control Name	Priority
CM-1	Configuration Management Controls	P1

Statement

Configuration Management is a process for maintaining consistency of system's performance, physical and functional attributes with its requirements, operational and design. The purpose of Higher Education configuration management measures is to provide guidance to maintain security measures against all physical and logical platforms to keep confidential information. The purpose is also describe the needs to configure new platforms securely and maintain security for platforms and its associated software.

The HEIs shall establish their configuration management policies and procedures. These procedures will support Institutions to manage risks raise due to system changes and impacting HEIs system and configuration settings, and system security settings

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute or Network Administrator should make sure that information system is using correct versions of policies and procedures and that formal mechanisms has been developed to implement new policies and procedures. The Head of the Institute or Network Administrator also shall develop configuration management system, document and circulate it. It should also review/update policies and procedures at regular interval minimum annually. If there is a change required in configuration management then the possible procedure should be adopted to update and implement it.

Control Number	Control Name	Priority
CM-2	Baseline Configuration	P1

Statement

The Higher Education Institutions must develop, maintain and document baseline of configuration of its systems. The baseline of configurations are required to be updated as and when it is needed.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of Institute or Network Administrator shall develop, maintain and document current baseline of the configuration. When there is change required in existing system, risk assessment must be carried out during changing process and baseline configuration has been defined adequately.

Control Number	Control Name	Priority
CM-3	Security Impact Analysis	P2

Statement

The Higher Education Institutions are required to analyze the changes in the information system of the Institute to get the impact of the security before the implementation of the changes.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Institute shall develop a mechanism to analyze all information system or to determine change in the security control due to change in the system configuration. All changes in the system must be reviewed in the light of risk assessment methodologies so that before completion of the changes, potential security impact may be documented.

Control Number	Control Name	Priority
CM-4	Least Functionality	P1

Statement

All IT assets of the Higher Education Institutions are required to be restricted the information system to specific and essential ports, protocols and services by implementing least privileges functionality.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Head of the Institute or Network Administrator shall review the information system periodically at least once in a month to find and eliminate superfluous functions, opened ports, unused protocols, and services. The Head of the Institute shall make sure compliance with all ibid requirements.

The Network Administrator shall identify/find all programs that are authorized to be used in IT environment. Furthermore, the Network Administrator also shall update

the list of the changes that are made in privileges and reviewed at least once in a month to make sure that current status of the list. The Network Administrator in addition to this, shall also prepare the list of those programs that are not authorized to be used. By default, the Network Administrator shall maintain the most restrictive permissions in the system.

Control Number	Control Name	Priority
CM-6	Information System Component Inventory	P1

Statement

The owner of the resources / Head of the Institute shall develop, maintain and document all IT assets including software, and removable media that are in use and even out of order accurately. The inventory shall include detail of each item, inventory must be reviewed and rechecked and reconciled annually.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☒ Compute
☐ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute shall make sure that all IT / information assets are properly entered in the inventory register along-with relevant ownership information. The owner of the assets shall also update inventory of information assets and consider updating of inventory as part of assets installations and removal. The HEIs shall also develop automated mechanisms to monitor and detect unauthorized hardware and software within the information system and if found then disable network access, isolate the components and sent notification to the relevant officials.

Control Number	Control Name	Priority
CM-7	Software Usage Restrictions	P2

Statement

The installation of purchased software on University information assets and its use must be in accordance with license agreement.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator shall use software of the Institutions keeping in view contract agreement with owner of the software, comply with copyright laws and not share such documents and protect from unauthorized distribution.

Control Number	Control Name	Priority
CM-8	User Installed Software	P1

Statement

The Higher Education Institutions shall establish, document and impose a policy that governs the installation of software by the staff members and faculty members. The Network Administrator should monitor the compliance of ibid policy and review it annually. The Network Administrator shall also develop a policy to manage software changes and must be monitored at regular interval to make sure that only approved software are operational and that no other software has been installed and operated.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The students of the Institute should be prohibited to install software, whereas, the faculty and staff members are allowed to install software to meet their requirements. However, the Network Administrator must remove the software that are slowing down the performance of the information resources.

Authority: [79] [93] [94] [104] [20] [21] [107] [108] [24] [25] [111] [95] [24] [6] [20] [23]

6.2.6 **Contingency Planning**

Unexpected events occur that adversely affect information systems containing Institute information and, therefore, disrupt education operations. The Higher Education and Information Security Officers of the Institutes must recognize the requirements to define contingency plans, which give way forward to maintain education operations at some level.

The formulation of data backup, disaster recovery, emergency operating, testing of contingency plans, auditing of these plans, applications and data criticality are the essential things to become contingency plan more successful. Each of these sub-plans can be truly exclusive to the individual entity depending on the size, complexity, location, and technical considerations. Contingency Planning policy and procedure module provides the mandatory steps necessary to identify or initiate the development of each component.

Suitable planning and testing should be carried out to ensure that in the case of critical event, educational environments are restored and maintained to meet the education requirements of the Higher Education. To facilitate the effective restoration of systems and compliance with this policy, coordination between education units and Higher Education is required. This module / component of the framework covers the information system and cloud hosted environments.

6.5.6.1 Contingency Planning Controls

Control Number	Control Name	Priority
CP-1	Contingency Planning Controls	P1

Statement

Contingency Plan is a sequence of actions that are required to be followed in the case of preferred plan or present situation changes. The Higher Education establishes, document, maintain, monitor and implement plans for quick emergency instant response, initiate backup operations, and disaster recovery for Higher Education information system to make sure the availability of critical and non-critical information resources through implementation of contingency planning program. The purpose of instant control is to establish contingency planning policies,

procedures and regulations, and to manage risks that attacks due to the failure of system and assets disruptions.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

All Higher Education Institutions shall develop, document, maintain contingency plan for their Institutions and Institute resumption plan by defining the method to restore required operations of system in the case of failure. The said policy shall be disseminate, review and update every year and if there is a substantial change, that define the Institute requirements, it shall be addressed through Contingency Planning.

Control Number	Control Name	Priority
CP-2	Contingency Plan	P1

Statement

Adequately maintaining contingency plan is the part of Continuity of Operations and it plays a vital role to minimize the effects of natural disasters. Each Higher Education Institute shall develop, disseminate, review and up to date contingency plan and test it periodically to allow the information system to resume mission critical resource functions within stipulated time.

The following items are required to be included in the contingency plan:

1. Identify crucial missions and business functions
2. Contingency requirements against each mission and function
3. Provide alternate restoration plan, resources, recovery time, objectives and priorities
4. Document all activities including restoring all IT assets, applications and information system after disruptive failure

5. Occupant Emergency Plan (OEP) to rescue students, faculty and members in the case of emergency. Conduct OEP drill, review and update OEP at least annually
6. Define contingency roles and responsibilities and share their contact information
7. Distribute copies of contingency plan to the concerned personnel to implement and communicate it.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education Institution shall establish contingency plan, document, disseminate to focal personnel and also store its copy to another site.

Control Number	Control Name	Priority
CP-3	Contingency Training	P2

Statement

The Higher Education will arrange and provide contingency training to Institute faculty and staff members according to their assigned roles and responsibilities within 15 days of assuming a contingency responsibility and document it.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall train personnel to perform their contingency roles and responsibilities to deal any untoward situation with information system and also shall provide refresher training at least annually.

Control Number	Control Name	Priority
CP-4	Contingency Plan Testing	P2

Statement

The Higher Education must thoroughly examine and test the contingency plan such as tabletop test at least annually to evaluate the effectiveness of plan, review contingency plan test results and take corrective measures, if needed.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall test all contingency plans. All Institutes shall develop and implement test plan to make sure that all operations can restored. The Institute shall review plan results and take corrective measures, if required.

Appropriate testing of the disaster recovery plan will be tested at least annually. A formal report detailing the results will be prepared including lessons learned. Updates to the plan that are needed will be made at that time. Tabletop exercise must be carried out. Test results should be documented for future use.

Control Number	Control Name	Priority
CP-5	Information System Backup	P1

Statement

The Higher Education Institutions shall conduct backups of all students, faculty and staff members information stored in the information system and also conduct backups of system information as well. The backup of all information system documentation as well as security related documentation. The Network

Administrator must make sure that all backup devices are protected and their confidentiality, integrity, and availability is adequately maintained at storage location. The Network Administrator shall also test the capability of the backup devices to make sure that information could be recovered as needed.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

Risk management related decisions are required to be performed on all backups of systems. The Network Administrator shall review all backups, adequately test each backup device, perform test on backups, document all test results, review backup procedure annually and successfully and transported to an another site for storage.

Control Number	Control Name	Priority
CP-6	Information System Recovery and Reconstitution	P1

Statement

The Higher Education Institutions shall make sure that all procedures are opted to get the recovery and reconstitution of all the IT assets of the information system to get know about its state after disruption or failure. The backup restoration capability is required to be tested to ensure that information could be recovered within stipulated time as needed. Tabletop test shall be exercised to further make sure that data can be recovered from storage media, as required.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation
The Higher Education Institutions shall adhere all laid down procedures regarding recovery and reconstitution to allow the system to be recovered to a secure state after failure of the system.

Authority: [79] [81] [82] [83] [84] [86] [93] [94] [97] [95] [24] [6] [20] [23]

6.2.7 **Data Security & Information Life-Cycle Management**

Data and information security is a critical element in the maturity of information lifecycle management. As organizations adopt education models that provide employees, staff, students, partners and suppliers with greater access to confidential information, they create greater education opportunities and greater risks. The risk of cyber terrorism and data theft have increased the need to protect Institute information. Education Institutions understand increasingly and respond to this need. However, a recent survey by Sun Microsystems showed that most managers and technical staff assess their security operations as not fully integrated with storage management policies. Organizations that have medium data centers (at least 50 terabytes of disk) have a much higher degree of integration than those with smaller data centers. Organizations that have large data centers (at least 100 terabytes of disk) are categorized by linking storage security policies to network security policies. The technical staff, who are more likely than other groups of participants to have a detailed understanding of the current state of your organization, the storage rate and network security integration policy is low This is worrisome, given the recent huge efforts to create network storage environments. No single third party organization can offer all requirements to meet these needs.

Information Lifecycle Management is a justifiable storage strategy that stabilities the cost of storage and information management with Institute value. Well executed Information Lifecycle Management strategies should lead to more flexible Institute, reduce Institute risk and reduce storage and storage management unit costs. Storage security from Information Lifecycle Management perspective focuses on protecting data from unauthorized access, destruction or tampering. This approach includes preventing unauthorized persons from accessing any content, allowing trusted people access only to content that their role requires, and preventing them from misusing or damaging the content. Information Lifecycle Management acceptance efforts without acceptable storage security can compromise data integrity and increase the threat of

disclosure to wrong parties. However, the access of knowledge workers to the data is necessary to create a strategic advantage. The successful design and implementation of storage security must balance the critical requirements of access and protection. The specialization in storage security has become important increasingly in recent years. Institutes allow access to data from outside their traditional environment, expand access by implementing network storage and create potential exposure through the use of IP-based storage networks. Changes in government regulations also intensify the focus on storage security. Data must be properly maintained, whether it is stored in storage systems or used effectively within or outside the data center. It is important to focus on external and internal security threats. It is also necessary for organizations to consider the educational value of their data to establish or improve their security practices, although many organizations do not. Storage networks have matured to a point of complexity that require an additional perimeter, as well as internal security services to ensure data integrity.

6.5.7.1 Data Security & Information Life-Cycle Management Controls

Control Number	Control Name	Priority
DS-1	Data Security & Information Life-Cycle Management Policy & Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of Data Security & Information Life-Cycle Management Policy and Procedures, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of Data Security & Information Life-Cycle Management Policy and Procedures and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☒ Compute

Cloud Service Delivery Model

☒ SaaS ☐ PaaS ☐ IaaS

☐ Storage ☐ Application ☒ Data

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the Data Security & Information Life-Cycle Management Policy and Procedures.

Control Number	Control Name	Priority
DS-2	Classification	P2

Statement

The classification of the data is required to sort it out. Therefore, the data must be classified according to data classification of the owner of the data, second the type of data and its sensitivity.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☐ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☐ PaaS ☐ IaaS
☐ Storage ☐ Application ☒ Data

Implementation

The Network Administrator of the Institute shall classify the data and its objects according the classification assigned by the owner of the data and it shall be based on file type, data type and its sensitivity. Furthermore, the third-parties also should be restricted to adhere data classification instructions.

Control Number	Control Name	Priority
DS-3	Ecommerce Transactions	P2

Statement

The Higher Education Institutions shall secure the data that it will traverse public network from fraudulent activity, viruses, malware, Trojans, unauthorized disclosure and modification and shall appropriately also be classified.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☐ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator of the Institute shall protect the data of the Institution that shall transverses public network and also should be classified.

Control Number	Control Name	Priority
DS-4	Handling / Labelling / Security Policy	P2

Statement

Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☐ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.

Control Number	Control Name	Priority
DS-5	Ownership / Stewardship	P2

Statement

The Higher Education Institutions shall designate the data with stewardship, defined responsibilities, document, review, and update as necessary and communicate to concerned personnel.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☐ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☐ Compute
☐ Storage ☐ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☐ PaaS ☐ IaaS

Implementation

The Network Administrator of the Institute shall designate the data with stewardship by keeping in mind the defined responsibilities, document it, review and update it at specified interval or necessary.

Authority: [93] [94] [95] [24] [6] [20] [23] [98] [99] [100] [101] [102] [103]

6.2.8 Identification and Authentication

In order to make sure the security and integrity of Institute and individual, the Information Security Officer in collaboration with Network Administrator must formulate and implement effective access control policies. In this framework, access control policies are already defined to protect the institute resources from unauthorized disclosure.

Authentication is a way to securely identify the system users. The Information Security Officer in collaboration with Network Administrator shall determine which authentication method is most suitable among the available methods for a particular system. However, the staff members and students of the Institute are strongly encouraged to use the authentication services of the Institute rather than use by default configured system authentication methods. The Institute identification and authentication service is more consistent instead of other authentication services.

The Information Security Officer is responsible for ensuring that all the staff member and students of the Institute are meeting minimum security requirements defined in this framework. This module addresses the policies, procedures and rules set forth by the Institute to implement the Identification and Authentication controls. The policies, procedures and rules defined in this module are applicable to those who used, managed, or operated the system, contractor, third party agency, or any other organization attached with the Institute. The procedures defined herein are also applicable to all staff members and students that will care the operations and assets of the Institute.

This policy module provides Institute security policy requirements for the user identification and authentication which is obligatory to protect an access to Institute information and systems and also critical education processes.

6.5.8.1 Identification and Authentication Controls

Control Number	Control Name	Priority
IA-1	Identification and Authentication Policy and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of the identification and authentication policy, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of the identification and authentication policy and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the identification and authentication policy.

Control Number	Control Name	Priority
IA-2	Identification and Authentication (Organizational Users)	P1

Statement

The Information System of the Institute must uniquely identify and authenticate each student, faculty and staff and other approved users of the Institute before granting access.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

Each student, staff and faculty member of the Institute shall be assigned unique identifier. The identification process must be completed before granting access to system. The Network Administrator is required consider following.

1. The Institute's Information System must be capable to authenticate privileged accounts using multifactor authentication.
2. Non-privileged accounts also must be authenticated by using multifactor authentication.
3. The Institute's Information System must be capable to handle replay attack.
4. The Institute's Information System must have capability to verify Personal Identity Verification (PIV) credentials.

Control Number	Control Name	Priority
IA-3	Identifier Management	P1

Statement

The Higher Education Institutes shall manage all identifiers, e.g. user names, groups, roles, access controls, usage limitations, devices for either IT systems to include the following:

1. The Network Administrator must make sure that roles and responsibilities of the students, staff and faculty members are clearly defined.
2. The Network Administrator must ensure that similar accounts cannot be reused.
3. The user accounts that are being used for a period of 30 days, are automatically disabled.
4. Privileged accounts shall be disabled automatically after 10 days of inactivity.
5. The user name must identify the type of its role of account.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☐ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education Institutions are required to manage identifier, modify it as user can change its role and or left the Institute. The Network Administrator must assign a unique identifier to each user and also manage its uniqueness permanently. The devices operate in Information System also must be assigned a unique identifier.

Control Number	Control Name	Priority
IA-4	Authenticator Management	P1

Statement

The Higher Education Institutions must manage authenticator in the following manners:

1. All passwords that are being used, are required to use complexity. The password must be consisted of alpha numeric, special characters, numbers, upper case and lower case.
2. Password must be configured in such a manner that it cannot be reused.
3. Password is required to be changed after every 90 days.
4. Tokens and certificates used then they have to meet the requirements.
5. Verify identity of each individual and device before making it as a part of the Information System.
6. Establish initial authenticator duly approved by the Head of the Institute.
7. Make sure that initial authenticator has sufficient capability for his planned use.
8. Review and update authenticator annually and as necessary.
9. Change authenticator for accounts when membership of these accounts changes.
10. Apply required and suitable controls to safeguard the authenticator.
11. Define lifetime restriction on authenticator and also define condition for its reuse.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☐ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Institute manages system authenticators by initiating its content; establish its administrative procedures for distribution, define procedures in the case of lost, damaged, compromised and also methods to revoke authenticators.

Control Number	Control Name	Priority
IA-5	Authenticator Feedback	P2

Statement

The Information System must obscure feedback about authentication information gathered during authentication process to protect it from unauthorized access. The Network Administrator shall apply cryptographic modules for authentication.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☐ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information System of the Institutes must configured to mask all passwords entered in the system. The failed login box should not indicate which part of the username and password is incorrect.

Control Number	Control Name	Priority
IA-6	Cryptographic Module Authentication	P1

Statement

The cryptographic authentication module of the Information System must meet the requirements of the applicable Pakistan federal laws, government executive orders, directions, policies applicable therein, prevailing standards, current regulations and user authentication guidance.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation
The encryption techniques and methods used in the Information System for authentication must meet the requirements given in the ibid statement section.

Control Number	Control Name	Priority
IA-7	Identification and Authentication (Non-Institutional Users)	P1

Statement
The Higher Education Institutes are required to recognize Non-Institutional users and temporary authenticate these users to Information System, keeping in view the access controls.

Applicability
This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☒ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**
☐ Physical ☒ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☒ Application ☐ Data

Implementation
The Network Administrator shall uniquely identify non-institutional users (guest) and grant access to information system after apply appropriate and required access controls.

Authority: [79] [80] [81] [82] [83] [84] [86] [92] [14] [15] [16] [93] [94] [95] [114] [115] [95] [24] [6] [20] [23]

6.2.9 **Incident Response**

The policies of the incident response are designed to help the Institutes to respond to reduce the effect of the cybersecurity incidents and the information of the staff and students is considered in the Institute. The response to security incidents has very important role in the Information Security Framework. The response to computer security incidents has become an important component of information technology (IT) programs.

The threats related security have become not only more numerous and varied, but also more harmful and disruptive. Therefore, an incident response capability is

necessary to detect accidents quickly, reduce losses and destruction, mitigate weaknesses that are exploited and restore computer services.

Information may be in the shape of Print, oral or electronic form, and systems have become essential parts of the infrastructure that supports Higher Education Institutions processes and innovations. This amplified dependence has taken place in the context of increased use of information for commercial purposes, technological complexity, information security and privacy risks, and ethical expectations that lead to more encouraging operational and financial consequences of disconnection, unauthorized exposure of information.

However, despite more vigilant efforts to reduce incidents, it occurs to threaten the security and privacy of information system. The process of preparation, prevention, detection, response and follow-up of these events to the institution has a significant influence in minimizing the frequency and severity.

Therefore, a consistent, efficient and effective identification, investigation and handling of prospect violations of information systems is therefore needed.

6.5.9.1 Incident Response Controls

Control Number	Control Name	Priority
IR-1	Incident Response Policy and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of incident response policy, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of incident response policy and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the incident response policy.

Control Number	Control Name	Priority
IR-2	Incident Response Training	P2

Statement

The Higher Education shall conduct incident response and reporting training to all its students, faculty and staff members along with their roles and responsibilities. This training shall be conducted at least annually or as changes made in the system as well as personnel changes occur. The staff and faculty members who are newly recruited in the Higher Education shall complete said training within 30 days after their joining.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall train its personnel in their incident response roles and responsibilities in respect of the information system and also offers refresher training courses of the said training annually.

Control Number	Control Name	Priority
IR-3	Incident Handling	P1

Statement

The Higher Education is required to maintain incident handling capacity to cope security incidents. All the Higher Education Institutions should have a procedure in place that describes the methods that shall be used in the event of incident. All the incidents handing procedures shall be documented, including incident detection and analysis, tools and techniques to handle the incident, opt procedures, containment,

eradication and incident recovery initialization procedures. Experience gained from incident handling activities shall be the part of incident response procedures, test and examine results and if changes are required then change incident handling procedure. The Network Administrator shall develop and document the list of the security incidents potentially affect the Information System.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall implement an incident handling capability of the Information System comprising of detection and analysis of the incident, tools and techniques to handle the incident, opt procedures, containment, eradication and incident recovery initialization procedures.

Control Number	Control Name	Priority
IR-4	Incident Monitoring	P1

Statement

The Higher Education Institutes shall minutely track and document all security incidents, including reason of the incident, vulnerabilities in the Information System due to which incident occur, status of the incident, information for forensics, detailed description and potential incidents connected with incidents.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall track and document all security incidents of the Institute on an ongoing basis.

Control Number	Control Name	Priority
IR-5	Incident Response Assistance	P2

Statement

The Higher Education shall provide incident response support through help desk which will provide assistance to the Institutes on handling of security incidents. The help desk personnel of the Higher Education should be adequately trained and should have to understand to help the Institute to resume operations of Information System and to handle potential security incidents.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education must constitute help desk for the concerned personnel of the Institute to offer their advice and assistance on incident handling at the time incident and reporting of security incidents. The instant support resource is an integral part of Higher Education's incident response capability.

Control Number	Control Name	Priority
IR-6	Incident Response Plan	P1

Statement

The Higher Education shall develop, document and review an incident response plan that has capability to handle incidents:

1. Provide Higher Education with a roadmap to implement its planned incident response
2. Describe the structure and incident response capability of the Higher Education

3. Provide an advanced approach regarding how incident response capability shall implement into the overall Institutions
4. Define existing reportable incidents;
5. Provide the ways to measure the capability of the incident response in the Higher Education Institutions.
6. Describe required resources and support required to effectively maintain incident response capability of the Institutes.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance			**Cloud Service Delivery Model**		
☐ Physical	☒ Network	☒ Compute	☒ SaaS	☒ PaaS	☒ IaaS
☒ Storage	☒ Application	☒ Data			

Implementation

The Network Administrator shall distribute copies of the incident response plan to the concerned IR personnel who are responsible to restore information system in the event of incident, regularly review incident response plan, updates it to manage system changes occurred during plan implementation and communicate updates to other concerned personnel, monitor incidents recovery, document incident recovery and results and finally safeguards the IR plan from unauthorized access.

Authority: [79] [80] [81] [82] [83] [93] [94] [116] [117] [118] [119] [97] [95] [24] [6] [20] [23]

6.2.10 **Infrastructure & Virtualization Security**

The vender and third parties goals are based on information technology to provide the best services at the lowermost possible cost. The challenges of maintaining worth, flexibility and maintaining healthy budgets cannot be easily overcome. More than ever, Higher Education Institutes need a strategy that allows them to manage vital infrastructure at the lowest possible cost and transform environment into a perfect level of performance. Virtualization is a key element of this strategy, and finding the right partner to manage infrastructure and development is another.

Managing Institute infrastructure can be redundant expense in Institute IT budget and internal resources.

6.5.10.1 Infrastructure & Virtualization Security Controls

Control Number	Control Name	Priority
IV-1	Infrastructure & Virtualization Security Policy and Procedure	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of Infrastructure & Virtualization Security Policy and Procedures, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of Infrastructure & Virtualization Security Policy and Procedures and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the Infrastructure & Virtualization Security Policy and Procedures.

Control Number	Control Name	Priority
IV-2	Audit Logging / Intrusion Detection	P1

Statement

Higher levels of assurance, retention and protection of audit logs and intrusion detection is required by adhering all applicable legal, regulatory compliance to detect suspicious network behaviour and file integrity anomalies. Furthermore, audit logging support in forensic investigation of security breaches.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Information Security Officer and Network Administrator shall develop audit logging and intrusion detection system by adhering applicable legal and statuary compliances to detect suspicious network behavior.

Control Number	Control Name	Priority
IV-3	Change Detection	P1

Statement

The integrity of all the images of virtual machines are required to be maintained. If there is any change required in the image of the virtual machine then change management procedures shall be adopted and it must be logged properly and alert must be issued. The third party shall communicate the change in image of virtual machine to the Institute through electronic method.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator shall adequately monitor the changes in the image of the virtual machine in the light of change management system and also restrict third party to communicate changes in the image of the virtual machine through electronic method to the Institute.

Control Number	Control Name	Priority
IV-4	Clock Synchronization	P1

Statement

The Information Security Officer shall use reliable external time source to synchronize the system clocks of all information processing systems located at the third party site to facilitate tracing and re-formation of activity timelines.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall configure reliable and mutually agreed time sources all relevant information processing systems to synchronize system clocks and to facilitate tracing and reconstruction of activity timelines.

Control Number	Control Name	Priority
IV-5	Information System Documentation	P1

Statement

The Higher Education Institutions shall prepare, plan and document the required number of resources, existing resources, required quality of services, up to mark performance in accordance with legal and statutory obligations. Forecast of future capacity shall also be prepared to reduce the risk.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall forecast the future capacity of information security resources required in both the Public and the Private Clouds to mitigate the risks.

Control Number	Control Name	Priority
IV-6	Vulnerability Management	P1

Statement

The Higher Education Institutions shall make sure that security vulnerability assessment tools related to virtualization technology are adequately implemented upon Information system of the Institute.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☒ Compute
☐ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall implement vulnerability assessment tools and techniques in the Information System of the Institute to reduce the potential risks.

Control Number	Control Name	Priority
IV-7	Network Security	P1

Statement

The Information Security Officer and Network Administrator shall make sure that Network Environment of the Higher Education Institutions and also virtual machines are configured in such a way to restrict and monitor traffic of the untrusted connections.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator is required to design and configure network environment and virtual machines in such a way that it monitors all traffic of trusted and untrusted connections. The configurations shall be reviewed monthly or necessary, documented with the justification of all the allowed services and permitted connections, protocols, ports and update if required.

Control Number	Control Name	Priority
IV-8	OS Hardening and Base Controls	P1

Statement

The Higher Education is required to provide only necessary pots, protocols and services to the students, staff and faculty members to meet the Institute requirements and provide all technical services at one place like antivirus, antimalware and logging etc. and also baseline standard operating system or template.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☐ Data

Implementation

The Network Administrator shall build standard template of operating system consisting of antivirus, antimalware, port scanner, vulnerability management tools, security scanning tools, and logging. The Network Administrator while building said standard operating system template shall make sure that only desired ports, protocols and services are enabled which meets the requirements of the Institute.

Control Number	Control Name	Priority
IV-9	Separation of Environment	P1

Statement

The Higher Education Institutions has to require to separate the Information System environment and classes to prevent unnecessary access to information assets. This separation may include boundary wall, authentication mechanism and clear segregation of duties of the personnel that who perform their duties.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute should make sure that the Information System environment and other environment are separated from each other and segregation of duties has been performed to avoid unauthorized access in the Information System environment.

Control Number	Control Name	Priority
IV-10	Segmentation	P1

Statement

The Network Administrator shall design and implement physical and virtual infrastructure and network components in such a way that Institute and students/faculty/staff members (tenants) access is adequately segmented based on the following parameters.

1. Establish segregation of tenants policy and procedure
2. Isolation of Institute sensitive data
3. Strong session that provide high level of assurance

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall design virtual infrastructure of the Institute in such way that no guest operating system may interfere into other guest operating system even cannot have access host operating system.

Control Number	Control Name	Priority
IV-11	VM Security - Data Protection	P1

Statement

Secured communication channels are required through implantation of cryptographic means when outsource the physical servers, applications and transfer data to Cloud Service Providers.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☒ Compute
☐ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall implement cryptographic means while communicating with the systems installed within the Institute and outside the Institute. The cryptographic means shall also be used while transferring institute data to public clouds, access applications installed on the public cloud and accessing physical and virtualized servers installed on Cloud Service Provider site.

Control Number	Control Name	Priority
IV-12	Hypervisor Hardening	P1

Statement

It is required to restrict the access on the system that has installed hypervisor management functions from the personnel who are not authorized and based on the principle of least privilege. Appropriate security and technical controls like two factor authentication, logging, auditing, firewalls shall be implemented.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator of the Institute is required to secure hypervisor management console and the systems that have virtualization hosting system by implementing relevant security and technical controls.

Control Number	Control Name	Priority
IV-13	Network Architecture	P1

Statement

The Network architecture diagrams with clearly highlight the critical and highly risk areas as well as flow of the information are required to be developed. Technical controls and defense-in-depth techniques shall be implemented for detection and immediate response in the case of any anomaly detected in the information system.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator of each Institute shall develop physical and logical architecture diagrams of the system which clearly highlights the critical areas and highly risky / targeted areas of the network. Relevant technical controls also shall be implemented along-with defense-in-depth techniques to mitigate the risks attack and take immediate response.

Authority: [93] [94] [95] [102] [98] [99] [100] [101] [103]

6.2.11 **Interoperability & Portability**

The capability to make components operate in the self-governing environment with minimal effort or zero effort is called interoperability. As the cloud adoption risks include safety, vender lock-in, censorship, law and service. Interoperability is one aspects of vender lock-in. Reducing interoperability problems also decreases the vender lock-in, which has very high risk rate. Interoperability solution approaches are an integrated approach: all cloud service providers agree to the same standard and approach. Where the cloud provider has a same model to map out other criteria, the federal approach: agreements between cloud service providers to share work semantics. Interoperability and portability issues can be resolved at all levels like storage, networking, software, data, information, application, platform, virtual machine and management. In a Higher Education cloud environment, interoperability issues arise at multiple levels.

If Portability and Interoperability are compatible then cloud compatibility solutions are provided. These are important considerations for cloud development and planning, because they together make sure cloud continuity and do so without change (through portability). When these two factors are not addressed between components, the potential result is malfunctioning associated with costly downtime of education continuity.

Portability and Interoperability should be considered if cloud migration is performed to public, private or mixed cloud publishing solutions. They are important elements that must be considered to choose a service model, regardless migration strategy is SaaS, PaaS and IaaS. If portability and interoperability are not adequately addressed in moving to the cloud, the benefits of moving to the cloud may not be realized. Ignoring these aspects of migration to the cloud can cause expensive problems or delays in projects due to factors.

6.5.11.1 Interoperability & Portability Controls

Control Number	Control Name	Priority
IP-1	Interoperability & Portability	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of Interoperability & Portability Policy and Procedures, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of Interoperability & Portability Policy and Procedures and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the Interoperability & Portability Policy and Procedures.

Control Number	Control Name	Priority
IP-2	APIs	P1

Statement

The vender-lock in is one of the Cloud Computing Risks. The customer is not able to transfer / migrate his data from one service provider to another. Therefore, standard APIs are required to be used to cater this risk and to ensure transfer / migration of data.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.

☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**
☐ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation
The Network Administrator is required to restrict the third-party to use open and publish APIs to make sure the support for interoperability and facilitate migration of data from one Cloud Service Provider to another without changing format of the data.

Control Number	Control Name	Priority
IP-3	Data Request	P1

Statement
The availability of the data from the Cloud Service Provider is mandatory as desired by the Institute. The Institute is required to make sure that CSP is making compliance of the Instructions of the Institute regarding availability of the data as per departmental-standard format.

Applicability
This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.
☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**
☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation
The Network Administrator is required to restrict the third-party to provide structured and unstructured data on the desire of the Institute according to industry-standard formats.

Control Number	Control Name	Priority
IP-4	Standardized Network Protocols	P2

Statement
The third-party is required to use secure authentication protocols and standardized secure network protocols for the import and export of data from Information System.

The third-party is also required to provide the details of applied protocols to Institutes and also details about interoperability and portability standards.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator is required to restrict third-parties to use secure protocols for the authentication, standardized network protocols to exchange data, and also shall make sure that third-party has provided the details of the protocols to ensure portability and interoperability of data.

Control Number	Control Name	Priority
IP-5	Virtualization	P1

Statement

The third-parties are required to use industry recognized virtualization standards and platforms to make sure interoperability. The third-parties shall document every change made in the hypervisor in use and make it available to the Institute for review.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall restrict third-parties to use only industry-recognized virtualization platforms and standards so ensure interoperability.

Authority: [93] [94] [95] [24] [6] [20] [23] [98] [99] [100] [101] [102] [103]

6.2.12 **Maintenance**

Network devices, servers, and other equipment need routine services and updates to work at maximum capacity, efficiently and safely. In the ongoing effort to reduce downtime in the Institute's network, it is essential for the Information Security Officer and Network Administrator to disconnect servers and equipment from the network for regular maintenance during specified periods. In addition to regular maintenance, services requiring intermediate updates may need additional scheduling considerations. When possible, all Institutes IT units will be consulted when scheduling moderate updates to the oldest, which will involve contacting Institute IT units and the entire campus community for planned master reductions. This module specifies the Higher Education Institute policy for scheduling service outages so that routine / regular maintenance may be achieved to make sure system stability.

6.5.12.1 Maintenance Controls

Control Number	Control Name	Priority
MA-1	System Maintenance Policy and Procedures	P1

Statement

The maintenance of all IT assets of the Institute ensures that these assets are able to be used and also ensures the confidentiality, integrity, validity and reliability of the equipment. The Higher Education shall develop, document, circulate, review, and update policies as necessary and procedures at least annually or at the time of significant changes are required regarding maintenance for information system.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☐ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information system maintenance policy that addresses purposes, defines the scope of maintenance, roles and responsibilities of personnel, management commitment, defines coordination among departments of the Institute,

and compliance; procedures to implement maintenance policy and its associated controls.

Control Number	Control Name	Priority
MA-2	Controlled Maintenance	P2

Statement

The Higher Education shall establish a procedure to send IT equipment to off site for repair and maintenance as necessary. Before sending repairable equipment to off site for maintenance, a process is required to be established that defines the authorization for repair. The Network Administrator shall maintain inventory of the all the IT equipment that are sent for repair after the issuance of the formal approval letter. All potential impacted security controls are required to be verified. Any equipment that has sensitive information which cannot be repaired, must be destroyed through adopting rules and procedures.

The Institutions shall schedule, document, implement and reviews records of repair and maintenance of all the IT equipment of the Information System in accordance with vendor specifications and requirements. The Network Administrator should:

1. Prior repair / maintenance of IT equipment, get approval of the Head of the Institute, monitor all activities, whether it is performed in Institute or vender site.
2. Must ensure that only authorized personnel has granted access to remove the component from Information System of the Institute for maintenance and repair.
3. Sanitize equipment to make sure removal of information from connected media before transferring equipment to off-site for maintenance or repairs

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Institute should before repair or maintenance of equipment to off-site, the Institute shall properly assess whether data has adequately been removed from the equipment or its associated media. All electronic record shall be destroyed in accordance with the instructions given in description. Only restricted and trained concerned personnel shall be assigned equipment repair or maintenance. If the equipment has been contained personnel and confidential information, licensed software, mission critical information and it is not repairable, then it should be properly destroyed.

Control Number	Control Name	Priority
MA-3	Non-local Maintenance	P2

Statement

Remote / Non-local maintenance activities are those to whom vender / manufacturer shall access the Institute through broadband access or Virtual Private Network. The Head of the Institute shall approve and monitor all nonlocal maintenance activities; allow only nonlocal maintenance tools that are allowed in the procedure after considering security factors, Network Administrator shall apply strong authentication session between vender and Institute, create log of the nonlocal maintenance and activities and finally terminate session of the network after completion of nonlocal maintenance.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☐ Compute
☒ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education Institute shall authorize only legitimate remote session for nonlocal maintenance, monitor and log all activities, and control all remotely executed maintenance and diagnostic activities of the Information system, if employed.

Control Number	Control Name	Priority
MA-4	Maintenance Personnel	P2

Statement

The Higher Education shall establish a process for the authorization of the maintenance personnel and the list of the designated personnel with their roles and responsibilities, access rights granted to them, to ensure that only legitimate personnel are performing maintenance job on the information system, proper access controls are implemented on maintenance personnel prior maintenance. The Network Administrator shall personally supervise all the maintenance activities and personnel to log their activities.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute or Network Administrator shall allow maintenance of the Information System and equipment to only authorized personnel. In addition to this, the Network Administrator shall also perform the following:

1. Restrict the personnel who has no access of maintenance or appropriate security access on Information System.
2. Document the maintenance in the context of security.
3. Before initiating maintenance by the personnel who do not have required access authorizations, all volatile storage devices within the system shall be sanitized and all non-volatile media shall be removed or disconnected from the Information system and secured.
4. Develop and alternate security plan to safeguard the Information System in the event of equipment cannot be sanitized and remove from the Information System.

Authority: [79] [81] [82] [83] [84] [86] [93] [94] [97] [95] [24] [6] [20] [23]

6.2.13 **Media Protection**

The media is consisted of both the digital media (like hard disks, floppy disks, compact disk, tape drives, mobile devices, University Serial Bus drivers etc. and non-digital media like paper and microfilm. This module is included in the framework to safeguard all the types of media by all means. The media protection policies, procedures and rules that are given below must be reviewed at least in a year or as and when significant changes affect the security of the Institute and also when important modifications are required in the information system. The following sub-sections of this module describe the media protection requirements that the Institute must develop or commit to protect the privacy, security of confidential information and to prevent unauthorized use or misuse of Institute data.

6.5.13.2 Media Protection Controls

Control Number	Control Name	Priority
MP-1	Media Protection Policy and Procedures	P1

Statement

Media protection policies and procedures ensure that all type of removable Medias are properly secured. It allows continuous monitoring, reporting, and management of the media in the case of media loss, stolen or destruction. An inventory of all the media is required to be maintained and provided to the audit upon their request to get information about all the media used for storing and process institute information. Furthermore, media and its associated media protection policies and procedures should be documented, circulated for its compliance by the entities, and review and update current media protection policies and procedures, if necessary.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☐ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used for media protection.

These policies and procedures shall identify methods and requirements to restrain the unauthorized users to use information system media.

Control Number	Control Name	Priority
MP-2	Media Access	P1

Statement

The Higher Education Institutions shall make sure that proper control for the protection of Computer media to protect the security of the Institute's data has been adequately implanted. This control shall also apply on the data stored on the local system hard-disks, Institute server, remove-able media, external media, magnetic media and optical media like CDs / DVDs or disk drives.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☐ Compute
☒ Storage ☐ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education Institution shall make sure that Institute all types of media access are adequately restricted to prevent hard copy media from being lost and theft / stolen, or disclosed. Furthermore, all other types of media including electronic media, optical media shall be restricted to avoid unauthorized access. The students, faculty and staff members must also guide about the need of properly protection of sensitive information of the Institute against inadvertent disclosure.

Control Number	Control Name	Priority
MP-3	Media Sanitization	P1

Statement

The Higher Education Institutions shall properly sanitize information media, digital, optic, including paper before disposal or release for again use. All optical media storage devices including Compact Disks, Rewriteable CD, CD-Recordable, CD-ROM, optical disks i.e. DVD, Magnetic Optic disks should be destroyed by pulverizing, cross cut shredding or at least burning. Office shredders shall be used to shred the media that cannot be reconstructed. Media destruction shall be conducted through trained and authorized personnel. All disposal measures shall be identified before sanitization of any media. The record of all the media that destroyed shall be maintained. The record should comprise of the date of destruction, media contents, serial number of the media, types of media, type of media destruction technique, personnel performed destruction and the list of the witnesses at the time of destruction. The Institute media including paper material that is highlighted for destruction shall be secured.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☐ Compute
☒ Storage ☐ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Institute should before sale or transfer of data storage media and processing equipment to other institute or agent, the Institute shall properly assess whether data has been adequately removed from the storage media or its associated media. All electronic record shall be destroyed in accordance with the instructions given in the description. Only restricted and trained concerned personnel s shall be assigned media sanitization task. If the electronic media has contained personnel and confidential information, licensed software, mission critical information, then the storage media should not be transferred or sale and it should be properly destroyed.

In case, it is required to be transferred or sale, then the stored information shall be encrypted.

Control Number	Control Name	Priority
MP-4	Media Use	P1

Statement

The Institute must restrict the usage of personnel storage equipment, writeable removable media with the Institute information system and must use only Institute recognized defined types of media on Institute defined information systems.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☐ Compute
☒ Storage ☐ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education Institutes may restrict the use of handheld devices like mobile having storage capability with the information system of the Institute, based on documented risk management decisions.

Authority: [79] [80] [81] [82] [83] [84] [86] [92] [93] [94] [95] [120] [121]

6.2.14 Mobile Security

Mobile computing is a combination of various the most useful inventions of mankind on a single platform. While all these technological developments enhance mobile computing and people use mobile and handheld devices in everywhere, there are unprecedented security risks exist.

In the recent past, the graphs of the mobile cyber-attacks and malware attacks are increasing. The perception become greater in 2018; the risk of cyber-attacks with data fraud or theft is increased. The mobile internet connections and device for both the unprotected areas and large-scale malware can cause great economic and geopolitical confidence and damage to the Internet. The mobile applications become the main road for compromise. While the diversity of skills as well as mobile

convergence platforms obviously have a lot of opportunities for the users. It also provides a surface of large attack to malicious mobile users.

Therefore, mobile security must be the critical and necessary part of information or cybersecurity in general. The mobile security, is in fact the security of mobile computing, environments, software, application, systems and devices. To achieve a certain level of mobile security, is not an easy task. The asymmetry between attacking and securing mobile environments require seeing all. In short, mobile security must be a comprehensive process that require seeing the whole picture all the time.

6.5.14.1 Mobile Security Controls

Control Number	Control Name	Priority
MS-1	Mobile Security Policy and Procedure	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of Mobile Security Policy and Procedures, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of Mobile Security Policy and Procedures and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the Mobile Security Policy and Procedures.

Control	Control Name	Priority

Number		
MS-2	Anti-Malware	P1

Statement

The Higher Education and the Head of the Institutes shall arrange anti-malware awareness training specifically to handheld devices like mobile devices for the mobile users in their campuses and offices and also shall include in the third party information security awareness training.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☐ Data

Implementation

The Network Administrator shall design Anti-malware awareness training program for the mobile users of the campus and Head of Institute shall bind the third party to include information security awareness training in their training program.

Control Number	Control Name	Priority
MS-3	Application Stores	P2

Statement

The Higher Education and its Institutions have to develop a list of approved applications stores as acceptable for mobile devices to store and manage data.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☒ Application ☐ Data

Implementation

The Information Security Officer and Network Administrator in collaboration shall develop list of the approved applications that shall be used to store, access and manage data. The students, faculty and staff members shall use only approved applications to manage their data relates to Institution.

Control Number	Control Name	Priority
MS-4	Approved Applications and Stores	P2

Statement

The Higher Education and its Institutions have to develop a list of approved applications stores as acceptable for mobile devices to store and manage data.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☐ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer and Network Administrator in collaboration shall develop a list of the approved applications that shall be used to store, access and manage data. The students, faculty and staff members shall use only approved applications to manage their data relates to Institution.

The Information Security Officer shall also prepare a documented policy to prohibit the mobile users to install non-approved applications and the use of not approved application stores.

Control Number	Control Name	Priority
MS-5	Approved Software for BYOD	P1

Statement

Buy Your Own Device (BOYD) technology shall be adequately designed, documented and implemented in the Higher Education Institutions to embrace the technology trends, encourage students, staff and faculty members to get benefits from their devices by participating in BOYD program.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☒ Application ☐ Data

Implementation

The Network Administrator of the Institute shall develop BYOD policy and prepare awareness training program by clearly stating the number of approved applications, list of application stores, and relevant application extensions and plugins used for BYOD usage.

Control Number	Control Name	Priority
MS-6	Mobile Awareness and Training	P2

Statement

The Information Security Officer shall prepare a documented mobile device policy comprising of every type of definitions of mobile device, and Institute network acceptable usage and general requirements for all kinds of mobile devices. The Network Administrator shall communicate the said policy and the requirements through the Institute training program.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☒ Application ☐ Data

Implementation

The Network Administrator shall establish Mobile Awareness Training program after developing documented policy which should clearly state acceptable usage of Institute network and requirements of the all kinds of mobile devices.

Control Number	Control Name	Priority
MS-7	Cloud Based Services	P1

Statement

The Information Security Officer shall prepare a documented cloud based services security policy consisting of BOYD pre-approved mobile usage policy and storage of

Institute data. The Network Administrator shall communicate the said policy and requirements through the Institute training program.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☒ Data

Implementation

The Network Administrator shall establish cloud based services policy that all cloud based services accessed through BOYD shall be pre-approved for the usage and the storage of data.

Control Number	Control Name	Priority
MS-8	Compatibility	P1

Statement

Because of different categories and variety of mobile operating systems, their hardware and their restrictions, compatibility issues arise. The Higher Education is required to resolve the compatibility issues which cause security issues of the mobile devices.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☒ Application ☐ Data

Implementation

The Information Security Officer and Network Administrator shall develop a standard documented application validation process that shall check compatibility issues of the mobile devices that have Higher Education applications.

Control	Control Name	Priority

Number		
MS-9	Device Eligibility	P3

Statement

The Chief Security Officer is required to develop, document, and implement mobile and other handheld devices eligibility requirement to use BOYD.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☐ Data

Implementation

The Information Security Officer and Network Administrator shall develop the BYOD policy that will define device and entitlement requirements to permit for BYOD usage.

Control Number	Control Name	Priority
MS-10	Device Inventory	P3

Statement

The Head of the Institute and its Network Administrator are required to develop and maintain inventory of the mobile devices of the Institutes used to manage data of the Institute and also shall be responsible to update inventory monthly or as necessary.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☐ Data

Implementation

The Information Security Officer and Network Administrator shall maintain an inventory of all the mobile devices of the Institutions that are used to store, access

and manage data and this inventory shall be kept maintained and updated monthly. The inventory shall be consisted of version of the operating system, its patch level, functioning/lost/decommissioned status and status about allowed / approved for the usage of BOYD.

Control Number	Control Name	Priority
MS-11	Device Management	P2

Statement

The Information Security Officer and Network Administrator are required to develop, document and implement a centralized mobile device management system that shall be installed in all the mobile devices of the Institutions that are should be used to store, process, retrieve and manage Institute data.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer and Network Administrator shall develop, document, review, update and implement a centralized mobile device management application for the mobile devices owned by the Institutions and used to store, access, retrieve and data of the Institution.

Control Number	Control Name	Priority
MS-12	Encryption	P1

Statement

The Information Security Officer and Network Administrator are required make sure that all the mobile devices are owned by the Institute, the staff and the faculty members are using encryption on the sensitive data of the Institute.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.

☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☒ Data

Implementation

The Information Security Officer and Network Administrator shall develop, document, review, update and enforce encryption policy on all the mobile devices of the Institutions to use store sensitive data of the Institute in their mobile device after using appropriate encryption.

Control Number	Control Name	Priority
MS-13	Jailbreaking and Rooting	P2

Statement

The Information Security Officer shall make sure through developing a policy and procedure to prohibit the circumvention of existing security measures installed & configured in the mobile devices and also shall enforce detective controls to monitor violation of security controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Information Security Officer and Network Administrator shall develop, document, review, update and enforce jailbreaking and rooting avoidance policies as well as procedures on the on all the mobile devices of the Institutions. It should also enforce the prohibition through detective controls.

Control Number	Control Name	Priority
MS-14	Lockout Screen	P2

Statement

The mobile devices used by the students, staff and faculty members are required to be configured in such a manner that their screen automatically lockout.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☒ Application ☐ Data

Implementation

The Network Administrator shall configure automatic screen lockout in the mobile devices of the Institutions and during security awareness training, educate the users of the mobile devices especially uses using BOYD to configure their screen lockout setting to automatic.

Control Number	Control Name	Priority
MS-15	Passwords	P1

Statement

The Higher Education must implement existing Password policies and control to the mobile devices of the Institutions, restrict third party to opt the same policy for their employees assigned Institute tasks, and also enforce said the policy to the devices approved for BOYD usage.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☒ Application ☐ Data

Implementation

The Network Administrator shall restrict mobile users of the Institutions to adhere with the password policies and procedures and also restrict them to change password / pin-code without following formal procedure laid down by the Institute. The devise uses BOYD shall also be restricted to implement password policy.

Control Number	Control Name	Priority
MS-16	Backup Policy	P1

Statement

The Information Security Officer shall develop backup policy to the mobile devices of the Institutions and the mobile devices that are allowed to use BYOD. The mobile users of the Institutions and BYOD shall take backup of the data on daily basis or necessary, shall not be allowed to use unapproved applications stores, approved antivirus and anti-malware application.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☒ Compute
☐ Storage ☒ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall restrict mobile users of the Institutions and the mobile devices of the BYOD to use approved backup application to take daily backup of the data. The other should not be allowed to use unapproved applications and application store. The antivirus and antimalware shall be installed on all the mobile devices.

Control Number	Control Name	Priority
MS-17	Security Patches	P2

Statement

The Information Security Officer and Network Administrator has to make sure that all the mobile devices of the Institutions and the devices using BYOD program have been installed accordingly latest available security patches.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance			**Cloud Service Delivery Model**		
☐ Physical	☒ Network	☒ Compute	☒ SaaS	☒ PaaS	☒ IaaS
☐ Storage	☐ Application	☐ Data			

Implementation

All the mobile users of the Institutions and users of BYOD program should install latest available security patches on their mobile devices.

Authority: [24] [6] [20] [23] [101] [102]

6.2.15 **Personnel Security**

One of the main responsibilities of the Institute is to protect the staff and students of the Institute. Traditionally, it was understood that the Institute security was meant for the protection of the Institute from other threats, risks and attacks from outsiders. In the recent decades, the threats have been increased and Institute have to implement various means to protect the staff and students of the Institute.

To protect Institute security, the Higher Education must implement a series of preventive security measures. Some of these are about to staff, Adhoc employees, students, or contractors in sensitive or critical jobs. All of them may be considered under the personnel security.

Government employees, and persons working in sensitive infrastructure can receive a range of sensitive assets and are at the risk because of a wide range of threats. These threats and risks can be related to terrorism, spying, vandalism, or serious organized crime, but vulnerabilities can also arise from unsatisfied people who may try to misappropriate or damage assets they have access to. Similar considerations can be applied to Pakistani citizens who hold sensitive positions in national organizations.

The purpose of personnel security controls is to confirm the identity of persons (employees and contractors) and to provide a level of security in terms of reliability, integrity and reliability. Although personnel security has no complete mitigation capabilities, but it is reasonable precaution to properly identify people. Whereas risk assessments indicate that thresholds are met, they allow verification of official

sources and other sources of data that can indicate whether people can be affected or pressed, which may result in the abuse of their positions or if there is any other reason that prevents people from accessing sensitive assets.

6.5.15.1 Personnel Security Controls

Control Number	Control Name	Priority
PS-1	Personnel Security Policy and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of personnel security policy, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of personnel security policy and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the personnel security policy.

Control Number	Control Name	Priority
PS-2	Position Risk Designation	P1

Statement

All Higher Education Institution's employees and third the parties which have access information resources of the Institutions should agree with the Institute security policies and procedures revised time to time prior to for grant of access to Higher Education Information System.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☐ Student ☒ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Higher Education should establish screening criteria for all those applicants who applied for security positions and HR wing should designate security positions subject to their screening through agencies.

Control Number	Control Name	Priority
PS-3	Personnel Screening	P1

Statement

The Higher Education's Human Resources Department shall be responsible for screening and background check of all personnel screening as part of their recruitment process.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☐ Network Admn.
☒ Faculty Member ☐ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☒ Data

Implementation

The Higher Education shall uses background checks as a way of verifying potential employees as part of recruitment process.

Control Number	Control Name	Priority
PS-4	Personnel Termination	P1

Statement

The Higher Education Institutions shall upon termination of personnel employment disables his/her access to information system immediately. The personnel who has

passwords of the Information system, must be changed immediately. All types of authentication cards are required to be returned. The Institute conducts exit, retrieves all security-related Institute information through a checkout process. The Institute shall terminate all authenticators associated with the employee.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☐ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☒ Data

Implementation

Faculty and staff access of the Institute to Information System shall be cancelled upon termination of employment immediately. Information Security accounts of the individual shall be revoked and retrieve all information security related properties from the individual.

Control Number	Control Name	Priority
PS-5	Personnel Transfer	P1

Statement

The Head of the Institute or Network Administrator shall review all logical and physical access of the individual to information system of the Institute when individual reassigned or transferred to other position of the Institute, initiate reassignment process upon transfer, modify access authorization according to reassignment / transfer and document it.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☐ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☐ Storage ☐ Application ☒ Data

Implementation

The Head of the Institute and Network Administrator should review access privileges on a periodic basis or whenever job responsibilities of the individual will change.

Control Number	Control Name	Priority
PS-6	Access Agreements	P1

Statement

All the Higher Education employees and students must be see the rules, policies and procedures of the Higher Education relating to Information Security HR on boarding process. Students, staff members and faculty members agree to policy by acknowledging the code of conduct. Guest users are also required to agree and sign requesting form.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☐ Compute
☐ Storage ☐ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The students, staff members and faculty members must sign access agreement of the Institute prior granting access to the Information system.

Control Number	Control Name	Priority
PS-7	Third-Party Personnel Security	P1

Statement

The Higher Education shall restrict third parties to establish personnel requirements, document, and monitor for compliance. The third party and its vender shall monitor personnel security requirements of the Higher Education.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The third party should be restrict to adhere Higher Education third-party personnel security requirements.

Control Number	Control Name	Priority
PS-8	Personnel Sanctions	P1

Statement

The Higher Education and its Institutions shall establish formal sanction process for the personnel comprising of the formal notification of initiating of the formal sanction process, the reason of the sanction and the person approved about the sanction.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☐ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The HR in conjunction with the Head of the Institute will maintain and support formal sanction program.

Authority: [79] [80] [81] [82] [83] [93] [94] [95] [97] [122] [123] [95] [24] [6] [20] [23]

6.2.16 Physical and Environmental Protection

The physical security of the Institute is very important component of the framework wherein the Institute will protect and implement physical access, visitor access, incident management, emergency situation handling, emergency power supply, fire protection, water damage, temperature and humidity and access to transmission lines related controls are implemented to secure the Institute. Physical security of the devices and components is the primary control that has to be implemented in the

organization to protect the devices, buildings, accounts, and to restrict the third parties access. In the environmental protection, the Institute has to provide secure healthy working environment to the staff members and students of the Institute for their processing and stored information. The Head of the Institute, Higher Education, Information Security Officer and Network Administrator shall implement, document, review and update the Physical and Environmental Protection related policies, procedures and Principals in the Institute to safeguard the information and to avoid unauthorized access and disclosure of information.

6.5.16.2 Physical and Environmental Protection Controls

Control Number	Control Name	Priority
PE-1	Physical and Environmental Protection Policy and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of physical and environmental protection policy, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of physical and environmental protection policy and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the physical and environmental protection policy.

Control Number	Control Name	Priority
PE-2	Physical Access Authorizations	P1

Statement

The Higher Education Institutions shall plan, establish, approve, implement, maintain, monitor, review and update a list of the personnel along-with the authorized access to the information system and prepare and issue authorization credentials for the facility of the access.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator of the Institute shall develop and keep update the list of the students, staff members, and faculty members with their current authorization access facilities. The Network Administrator shall review the list every year and modify it according to their current roles and responsibilities and granted access facilities.

Control Number	Control Name	Priority
PE-3	Physical Access Control	P1

Statement

The Higher Education Institutions shall enforce physical access authorization of the IT Labs, server rooms, networking equipment and documentation by verifying each personnel access authorization prior to granting access to IT equipment. The Higher Education Institutions shall implement following physical access controls:

1. Audit logs of the physical access to server room / data center shall be maintained.
2. Monitor activities of the visitors when they request access to Information Security system of the Institute and visit the area where servers and networking equipment resides.

3. The entry and exit points of the most restricted area should be monitored through CCTV Camera and vigilant personnel should be appointed to verify identity of each individual.
4. The Visitors register should be maintained and is required to be reviewed at the end of each month.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Institute has require to verify each individual authorization access prior granting access to IT Lab, server room and networking facilities.

Control Number	Control Name	Priority
PE-4	Monitoring Physical Access	P1

Statement

The Network Administrator shall monitor physical access to Institute information systems, IT equipment and networking devices where Institute information is stored to detect and take action on physical security incidents. The Network Administrator also require to review all physical access logs monthly or upon occurrence of event. The review results and investigation reports are required to be communicated to the concerned personnel and Head of the Institute. Physical security Intrusion Detection Systems (IDS) shall be implemented to detect the attempts and breaches in the physical areas. Alarms for individual, document safety and other hazards are recommended to implement. Alarms are required to be communicated to Head of the Institute, Chief Information Security Officer, Incident / event management personnel and even Police Station if necessary.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP

☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☐ Application ☐ Data

Implementation

The Network Administrator shall develop, document, and review procedures to monitor physical access to IT facilities based on risk management decisions. Logs review and alerts of physical security is the part of monitoring.

Control Number	Control Name	Priority
PE-5	Visitor Access Records	P3

Statement

The Higher Education Institutions shall prepare, maintain, review, and update visitor access record throughout the year where IT Labs, server room and Networking equipment resides.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☐ Application ☐ Data

Implementation

The visitors of the Institutes might require access of the Compute labs, server room and networking equipment. It is required to enter their credentials at entry/ exit points and visit only at the specific time.

Control Number	Control Name	Priority
PE-6	Emergency Lighting	P1

Statement

The Higher Education Institutions shall maintain automatic emergency lighting system for the Institute Compute facility and should activate it at the time of power outage that should also cover emergency entry and exit evacuation routes.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute shall make sure that Institute has emergency lightning arrangement duly supported by separate power grid in the emergency entry and exit points. The Network Administrator shall ensure testing of emergency lightning arrangement weekly or atleast monthly.

Control Number	Control Name	Priority
PE-7	Fire Protection	P1

Statement

The Higher Education Institution shall deploy, maintain fire suppression and detection system in the Institute especially in the area where Information System resides and that fire protection system should be deployed duly independent uninterruptible power supply.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Institute shall arrange appropriate fire detection and suppression equipment in the Institute to protect Information System at the time of fire. The IT staff of the Institute shall be trained to respond fire suppression.

Control Number	Control Name	Priority
PE-08	Temperature and Humidity Controls	P1

Statement

The Higher Education Institutions shall maintain temperature and humidity level of the environment within the Institute especially in the areas where Institute critical data is maintained and continuously monitor temperature and humidity level and document it.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The production floor of the Institute must have controlled temperature and humidity level. The Head of the Institute in conjunction with the concerned personnel shall make sure the controlled environment to the Information System.

Control Number	Control Name	Priority
PE-9	Water Damage Protection	P1

Statement

The Higher Education Institution shall protect Information Systems from damage which may occur from water leakage by providing isolation valves that works properly.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☐ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation
The Institute IT Lab or other critical processing areas should be protected from the damage resulting from water leakage.

Control Number	Control Name	Priority
PE-10	Delivery and Removal	P2

Statement
The Institute shall authorizes, monitor, and control Institute equipment entering and exiting the facility. It should also maintain appropriate records of purchase items as needed.

Applicability
This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance
☒ Physical ☒ Network ☐ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model
☒ SaaS ☒ PaaS ☒ IaaS

Implementation
The Higher Education Institutions shall assess whether security to sensitive areas can be avoided by working with Institu5te third-party entities.

Authority: [79] [80] [81] [82] [83] [92] [15] [16] [97] [47] [48] [126] [127] [95] [24] [6] [20] [23]

6.2.17 **Planning**

The planning module is about the security planning for the Institute. Every quality security plan starts and ends with the policy that the management frames but due to non-technical management, Institutes cannot develop security planning.

Security planning states how issues should be addressed, how least expensive controls will be executed, frame principles that not contradict with the law, course of action, define requirements to be met, assign responsibilities, address legal compliance, frame issue specific policy, address specific technology, define what is right, what is wrong, the appeal process and the appeal process. The security policy also states what should be done to adhere with Institute formal and informal policies.

The security planning of the Institute must frame rules that protect the Institute's assets in issue specific and system specific manner.

Security planning is the initial and fundamental module of the framework because the Institute decided its way forward and course of actions to protect the Institute information and maintain integrity of the Information systems of the Institute.

6.5.17.1 Planning Controls

Control Number	Control Name	Priority
PL-1	Security Planning Policy and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update security planning policy and connected security planning controls of the information system that addresses purpose, define the scope of Security planning policy, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement Security planning policy and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon the changes required, that shall be used to complete a security plan. These policies and procedures shall identify methods and requirements to restrain the unauthorized users to use information system.

Control Number	Control Name	Priority
PL-2	System Security Plan	P1

Statement

The Higher Education Institute shall develop, circulate, review, safeguard, and update a security plan for Institute's information systems that:

1. It is stable with the Institute's enterprise architecture
2. It clearly describes the authorization limit for systems
3. It defines the operations of the system in respect of mission critical and processes
4. It provides supporting rationale of the security categorization of system
5. It describes operational environment of system and connections to other systems
6. It establishes an overview of the security needs for the system

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall develop, document, update and review it annually for appropriateness broad system security plan.

Control Number	Control Name	Priority
PL-3	Rules of Behaviour	P2

Statement

The Higher Education shall develop a set of rules personnel behavior, review annually, updates as needed, and makes readily available to personnel who requires access to the information system, their responsibilities and their conduct regarding information and its usage. These rules shall be displayed to the students, faculty members and the staff members through a system logon banner, all of these shall acknowledge that they have read, understand, and agree to adhere them prior to authorizing access to Information System understood.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance			**Cloud Service Delivery Model**		
☒ Physical	☒ Network	☒ Compute	☒ SaaS	☒ PaaS	☒ IaaS
☒ Storage	☒ Application	☒ Data			

Implementation

The students, faculty members and staff members of the Institute must agree to a satisfactory usage policies and procedures.

Authority: [79] [81] [82] [83] [84] [86] [97] [93] [94] [128] [129] [130] [95] [24] [6] [20] [23]

6.2.18 **Program Management**

It is core module of the framework where the information security program related plan are developed and executed. In program management, the Higher Education shall appoint Information Security Officer to monitor, maintain and implement the security plan developed herein. The estimation of the information security resources required to implement information security programs, budgeting of the information resources are the main concern in the program management which will be discussed under program management. Furthermore, in program management, the institute will clearly define action plans and milestone processes, discuss about information security inventory, information security measures for institute performance, risk management strategy, plans about the critical infrastructure, authorization of the security, dealing with inside threats, development of information security workforce, training of the personnel and contacts with other security groups.

6.5.18.2 Program Management Controls

Control Number	Control Name	Priority
PM-1	Program Management Policy and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of Program Management

Policy and Procedures, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of Program Management Policy and Procedures and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the Program Management Policy and Procedures.

Control Number	Control Name	Priority
PM-2	Information Security Officer	P1

Statement

The Higher Education shall appoint Information Security Officer, describe its role and responsibilities, provide him complete IT resources, training and certifications if necessary, to develop Higher Education Information Security System, implement, and maintain it to protect Higher Education and its Institution security all over the Punjab.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☐ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Higher Education shall designate an Information Security Officer to administrate Higher Education and its Institution's Information Security. The ISO shall be responsible to develop Information Security program, its policies and procedures, implement it in Higher Education and its Institution, ensure the compliance of Higher Education policies and procedures and monitor all information security relates policies.

Control Number	Control Name	Priority
PM-3	Information Security Resources	P1

Statement

The ISO and Network Administrator of the Institutes are responsible for budgeting and capital planning about for information security of the Higher Education Institutions. It will also ensure the allocation of sufficient number of resources for Information security. The ISO shall submit new services and equipment based on risk management decisions to the Higher Education for its consideration and approval.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall prepare both long-term and short-term plans to ensure priority of information security.

Control Number	Control Name	Priority
PM-4	Plan of Action and Milestones Processes	P2

Statement

The Higher Education and its Institutions shall make sure that action plans, including milestones for the fully deployment of Information Security, documented and executed. After completion of risk assessments, the information security officer will develop comprehensive plans to mitigate the identified risk.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute ☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The ISO will liaison with Network Administrators of the all the Institutions to get the updates of the identified risks, documents it, analyze it and prepare effective plan to mitigate risks.

Control Number	Control Name	Priority
PM-5	Information System Inventory	P1

Statement

All the Higher Education Institutions are required to maintain the inventory of information system and update it as item received / removed.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute ☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education Institutions shall automate inventory system of information system, conduct internal audit of the Institute at least every year to verify all IT assets and during risk assessment cycle.

Control Number	Control Name	Priority
PM-6	Information Security Measures of Performance	P2

Statement

The Higher Education Institutions shall develop and maintain reports on the results of IS measures of performance.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator shall prepare and review the reports of the measures for the effectiveness of the controls and will submit to Information Security Officer for review and comments.

Control Number	Control Name	Priority
PM-7	Enterprise Architecture	P2

Statement

The Information Security Officer of Higher Education shall develop, an enterprise architecture of the Information System by considering the information security, identified risks, threats, vulnerabilities, assets of the Institutions, staff and faculty members, students, the Higher Educations Institutions.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☐ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Information Security Officer shall review new information systems, information security systems as required and critical information systems monthly to ensure existing information security architecture of the Higher Education and its Institutions is appropriate and updated.

Control Number	Control Name	Priority
PM-8	Threat Awareness Program	P3

Statement

The Higher Education Institutions shall plan, develop, document and implement information security threat awareness program for the students, faculty member and staff members of the Institute. This program must have the capability of sharing of threats information among the Institutes and its users through email notification.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance			**Cloud Service Delivery Model**		
☒ Physical	☒ Network	☒ Compute	☒ SaaS	☒ PaaS	☒ IaaS
☒ Storage	☒ Application	☒ Data			

Implementation

The Information Security Officer and Network administrators shall maintain IT security threat awareness program to aware the students, faculty and staff members through emails, as required and monthly, about latest threats.

Authority: [79] [81] [82] [83] [84] [93] [94] [97] [116] [117] [118] [119] [131] [95] [24] [6] [20] [23]

6.2.19 **Risk Management**

Risk management processes include risk identification, assessment, prioritization, and identify the risk mitigation controls and techniques. The assessment of risks should include a systematic risk assessment approach and a process to estimate the intensity of the risks and the significance of the risk shall be calculated by comparing the estimated risks against criteria of the risk. The scope of the risk assessment can be estimated that Institute or parts of the Institute or particular portion of the information system or even certain components or services of the system will work. Risk assessment in the areas involving technological infrastructure also includes conducting vulnerability assessments to help identify risks. This risk and vulnerability assessment should be conducted at frequent intervals, especially if a step-by-step approach is chosen to ensure full and effective results. This will also make sure that ever-changing in security requirements or critical changes are evaluated.

The goals of this module are to identify potential threats before they trigger and manage them to reduce the impact they can have on the Information system. Risk management involves the pre-preparation of potential future events rather than responding to them as they occur.

6.5.19.2 Risk Assessment Controls

Control Number	Control Name	Priority
RA-1	Risk Assessment Policy and Procedures	P1

Statement

Risk assessment controls are developed to make sure that risk can be adequately assessed within the Higher Education Institutions, and that suitable mitigation controls can be implemented.

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update risk assessment of the information system that addresses purpose, define the scope of risk assessment policy, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement risk assessment and its associated controls. The purpose and goal of risk assessment can only be achieved if risk assessment is conducted effectively. The given below controls shall be implemented in the Higher Education Institutions to make sure that assessment has been conducted effectively and consistently.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete risk assessment. These policies and procedures shall identify

methods and requirements to restrain the unauthorized users to use information system.

Control Number	Control Name	Priority
RA-2	Security Categorization	P1

Statement

The Higher Education shall categorize information and information system in accordance with applicable laws, standards, guides, frameworks, executive orders, patents, policies and procedures, and regulations, documents each security categorization results and ensures that the security categorization decision is approved.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer shall properly assess the risks of each Institute's information system, the type of information and system criticality of each Institute 'system must be recognized and documented.

Control Number	Control Name	Priority
RA-3	Risk Assessment	P1

Statement

In the environment of all the Information System of Higher Education, a risk assessment is required to be conducted by the Institutions to assess the severity of the threat & risk that could result from the confidentiality, disclosure, destruction, integrity, modification and disruption. The results of the risk assessment shall be documented, transmitted to the other concerned personnel, reviewed at least annually and risk log is required to be updated as new risk arrives, or there is a significant change which is required in the system.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

A risks assessment of all the IT assets of the Information System are required to be perform regularly at least annually. The Network Administrator shall perform and monitor this process, share with Head of the Institute and other Institute to update their risk database, perform cost estimation and magnitude of the risk. The identified risk will be used to identify relevant controls to mitigate the risks and to help to protect the system. The results of the risk assessment shall also be used to develop Higher Education and Institute security plan.

Control Number	Control Name	Priority
RA-4	Vulnerability Scanning	P1

Statement

The Higher Education Institutes are required to scan vulnerabilities periodically through reliable vulnerabilities scanning tools in applications, all systems, information systems, physical infrastructure and employs screening tools and techniques. Such scanning shall enable interoperability between tools and automate parts as well as will identify software flaws, and its improper configurations.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Institute shall place all vulnerabilities scanning tools to satisfy this control.

Authority: [79] [81] [82] [83] [84] [86] [97] [93] [94] [128] [129] [130] [95] [24] [6] [20] [23]

6.2.20 **Security Assessment and Authorization**

Security assessment and authorization are the measures that may be implemented to protect students' information and Institutes' assets. Assessment and authorization have two-step processes that make sure the security and privacy of information systems. Assessment is related to evaluation, analyzation, and examination security controls that have already been pre-determined or stored in the information system of the Institute. The evaluation process is related to while comparing the current system state with the ideal standard state of the system. The assessment process always makes sure that security flaws are identified and accordingly suitable plans for mitigation of the risks and threats are in place. Authorization is something different, it is the process to agree to the residual risks linked with the continued operation of the Institute information system and approval to continue work for a specified limited period of time.

The assessment and authorization is consisted of several components like assessment and authorization policy, information system assessment, security controls for the risks, interconnect security agreement to make system more secure, plan of action and milestone, certification letter and accreditation letter, all these components are integrated with one another and form a comprehensive framework.

6.5.20.2 Security Assessment and Authorization Controls

Control Number	Control Name	Priority
CA-1	Security Assessment and Authorization Policies and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of Security Assessment and Authorization Policies and Procedures, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of Security Assessment and Authorization Policies and Procedures and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the Security Assessment and Authorization Policies and Procedures.

Control Number	Control Name	Priority
CA-2	Security Assessments	P2

Statement

The Higher Education Institutions shall conduct independent security assessment to validate that security controls have been adequately defined and is operating as per scope and implementation. Such security assessment shall be conducted annually or as required to ensure that controls are adequately implemented, operating as intended and their outcome is meeting security desire of the Institute. The Information Security Officer shall design security assessment plan and shall generate reports with the results of the assessment.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Information Security Officer of Higher Education shall ensure that every Institutions has security assessment plan, implementing it and producing reports for

further action. The Higher Education may hire the services of qualified 3rd party to review the security assessment.

Control Number	Control Name	Priority
CA-3	Information System Connections	P1

Statement

Each Higher Education Institute shall maintain the list of the users that are authorized to use the external systems, consisting of their roles, rights assigned to these users. The said list must be reviewed by the Network Administrator of the Institute and update it monthly or as required. The Network Administrator must monitor each information assets connections and then verify its security enforcement requirements.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator appropriately shall review all third-party connections to its Institute information systems and document it. The document should be consisted of individual information, purpose of connection, scope, third party information, connection use, duration of the connection, agreement and other useful information require to secure the connection. The Information Security Officer shall monitor the third party connections to make sure that security requirements are maintained.

Control Number	Control Name	Priority
CA-4	Plan of Action and Milestones	P3

Statement

The Higher Education and its Institutions shall make sure that action plans, including milestones for the fully deployment of Information Security, documented and execute. After completion of risk assessments, the information security officer will develop comprehensive plans to mitigate the identified risk.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The ISO will liaison with Network Administrators of the all the Institutions to get the updates of the identified risks, documents it, analyze it and prepare effective plan to mitigate risks.

Control Number	Control Name	Priority
CA-5	Security Authorization	P2

Statement

The Higher Education Institution should identify an owner for each asset and information system. The owner of the asset is require to authorize the information system before commencing operations.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall identify owners of the information resource. The ISO is responsible to authorize the implementation of Information System. The ISO and Network Administrator shall verify required security controls before system implementation.

Control Number	Control Name	Priority
CA-6	Continuous Monitoring	P2

Statement

All the Network Administrator of the Institutions and ISO shall plan a strategy for continuous monitoring. The monitoring strategy shall check assessment of the security controls, configuration management process and impact of change management. The monitoring strategy should be capable to demonstrate that implemented controls are functioning according to their desired results.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator of the Institutions shall deploy automated tools for real-time monitoring of the implemented controls, issue notification to concerned personal for appropriate response as any wrongdoing detected in the information system and vulnerability exploitation.

Control Number	Control Name	Priority
CA-7	Internal System Connections	P2

Statement

The Network Administrator of the Institute is required to document properly all internal connections of the Institute resources. This document should be consisted of Name of the both systems, type of connection, purpose of connection, MAC address of both systems, type of media and any other information required to be included.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance			Cloud Service Delivery Model		
☒ Physical	☒ Network	☒ Compute	☒ SaaS	☒ PaaS	☒ IaaS
☒ Storage	☒ Application	☒ Data			

Implementation

All internal connection of the Institute even with its sub campuses will be reviewed, properly documented, and updated periodically.

Authority: [79] [81] [82] [83] [84] [15] [16] [97] [116] [95] [24] [6] [20] [23]

6.2.21 Supply Chain Management, Transparency and Accountability

Reducing risk is one of the pillars of education success. A critical concern in any educational activity is the information security risks and threats in the information system of the Institute. Risk increases as the Institutes adopt new technologies. Risk management becomes an important part of every successful educational model to address threats and vulnerabilities. Security concerns are important factors in reducing risks by protecting Institute resources and intangible assets. The advent of supply chains that coordinate Institutions, personnel, activities, and resources increases risk crises.

Because of complex relationships with the third parties and venders of social, economic and industrial problems, risks occurs at different stages of educational processes, possibly because of the many types of security threats are caused by change in technology, social networks, budgetary constraints and internal policies. Risk recognition strategies include risk transfer to other party, avoiding risks, reducing negative impacts and accepting some or all of the consequences of a particular risk. Risk management goals are to reduce the impact of a crisis in a particular area. The advent of communication technology allows disparate Institutions not only to talk, but also to manage the supply chain of suppliers and customers. Because of supply chains, Higher Education Institutions can cooperate and coordinate their operations with other Institutions.

6.5.21.2 Supply Chain Management, Transparency and Accountability Controls

Control Number	Control Name	Priority
SM-1	Data Quality and Integrity	P1

Statement

The Higher Education and Head of the Institute shall inspect, make accountable, and work with their third parties to accurate their quality of data and remove errors as

well as associated risks. The Information Security Officer shall design and implement information security controls to mitigate information security risks related to supply chain management.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer shall coordinate with the third parties and venders and exchange experiences related to risk management to reduce the level of risk. Furthermore, implement supply chain related controls, least privileges, limited access and role and responsibilities.

Control Number	Control Name	Priority
SM-2	Incident Reporting	P2

Statement

Every organization has implemented incident management system in its organization as the party of the information system. Sharing of the information and experiences related to security incidents can enhance the security of both the organizations and also can support both the organizations to identify risks and its mitigation.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer should restrict third party or vender to share security incident information to all the connected parties through email, calls, SMS, or any other electronic methods.

Control Number	Control Name	Priority
SM-3	Network and Infrastructure Services	P2

Statement

For the third party or vender deal with the Institutions should implement business-critical, application and API designs infrastructure and systems components in accordance with the decided terms and conditions of the agreement and also build capacity as decided, provide services as prescribed and implement policies and procedures related to information security.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer while deciding terms and conditions of the service and the third party while designing and implementing decided terms and conditions of the agreement should make sure that all decided capacities, adherence with standards and certifications, and other network and infrastructure related conditions are fulfilled.

Control Number	Control Name	Priority
SM-4	Provider Internal Assessments	P3

Statement

The effective supply chain management cannot be complete without its formal internal annual review and assessment. The review include adherence of policies and procedures, measures to mitigate supply chain risks and metrics to evaluate other parties security.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Information Security Officer shall perform annual internal assessments of supply chain to get its effectiveness and security benefits.

Control Number	Control Name	Priority
SM-5	Supply Chain Agreements	P3

Statement

The Institutes shall develop agreements for their party services in such a manner that first it should secure the interest of the Institutions and not include any clause / condition that conflict the interest of the Institute. Furthermore, similarly, the Institute shall not accept any term and condition of service that does not secure institute interest.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Information Security Officer shall supply chain agreement keeping in view interests of the Institute.

Control Number	Control Name	Priority
SM-6	Supply Chain Governance Reviews	P3

Statement

The Institute shall review its risk management policies and procedures with their third parties and venders even with other Higher Education Institutions to make policies and procedures more consistent to identify as well as to mitigate the risks that inherited from other Institution supply chain management.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Information Security Officer and Network Administrator should corelate align Institute risk management system with other Institutions and partners to get the benefits of their experiences as well as identify risks associated with their information systems.

Control Number	Control Name	Priority
SM-7	Supply Chain Metrics	P3

Statement

IT Organizations develop metrics to gauge the performance of the system. Similarly, the Higher Education Institutions are required to develop Information Security Metrics as well as Supply Chain Metrics to know their adherence level through agreement and performance level of partners.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Information Security Officer and Network Administrator of the Institute should develop Supply Chain Metrics for the measurement of performance, effectiveness and acceptance level with the agreement.

Control Number	Control Name	Priority
SM-8	Third Party Audits	P3

Statement

The third-party and vender must provide their internal audit report to their customers so that they may satisfy themselves about the secured services they receives. The Institute should keep the record of the third party audit and reports for the use during reviewing the agreement.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Head of the Institute and Information Security Officer of the Institute must obtain audit copies and repots of their partners and consider their risks and threats while reviewing agreement.

Authority: [93] [94] [95] [24] [6] [20] [23] [98] [99] [100] [101] [102] [103]

6.2.22 System and Communications Protection

System and communication protection is very important module in the information security framework for higher education. It deals with the application Partitioning, Information in Institute Shared Resources, protection against Denial of Service attacks, protection of boundary, integrity and confidentiality of the transmission lines including wireless, cryptographic key management, protection of the cryptographic keys, protection of the data and information available publically, mobile device security, protection of the information at rest, ports and Input and Output devices and information system usage restrictions.

6.5.22.1 System and Communications Protection Controls

Control Number	Control Name	Priority
SC-1	System and Communications Protection Policy and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the

information system that addresses purpose, define the scope of System and Communications Protection Policy and Procedures, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of System and Communications Protection Policy and Procedures and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the System and Communications Protection Policy and Procedures.

Control Number	Control Name	Priority
SC-2	Denial of Service Protection	P1

Statement

The Network Administrator of the Institute shall deploy various information security controls to monitor effectively the attempts of denial of service so that action may initiate timely to maintain the availability of the network.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Information Security Officer and Network Administrator shall make sure that all Information Technology assets and resources, firewalls, routers, bridges, switches and other devices are protected against the denial of service attacks.

Control Number	Control Name	Priority
SC-3	Boundary Protection	P1

Statement

The internal and external boundaries of the Information System are required to be protected by using boundary protection mechanism.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☐ ISO ☒ HOI / Custodian ☐ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator should make sure that network services are operating effectively to protect the connectivity between Institute Information System resource and all the internet traffic is passing through firewall.

Control Number	Control Name	Priority
SC-4	Cryptographic Key Establishment and Management	P1

Statement

It is required to manage cryptographic keys within the information system. When asymmetric keys and Public Key (PK) certificates are used, the Network Administrator shall manage keys and measures.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☐ Compute

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

☒ Storage ☐ Application ☒ Data

Implementation

Cryptographic keys are required to be implemented in the Higher Education Institutions. The Network Administrator of the Institute will manage cryptographic keys using automated mechanisms duly supported by procedures. Network Administrator shall make sure that these keys are protected from disclosure and properly storage controls are implemented.

Control Number	Control Name	Priority
SC-5	Cryptographic Protection	P1

Statement

The cryptographic system implemented in the Information System of the Institute is required to be protected by using FIPS 140-2 or later validated cryptographic modules.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☒ Network ☐ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☐ Application ☒ Data

Implementation

The confidential information stored in the Institute portable devices, hard drives, removable media, optical media and others or non-Institute owned systems (including cloud) shall be protected through encryption with atleast 128-bit algorithm.

Control Number	Control Name	Priority
SC-6	Collaborative Computing Devices	P1

Statement

The Higher Education Institutions may collaborate with one another to exchange information and material. Therefore, the Institutions are required to secure their remote connections and prohibit remote activation unless approved by the Network Administrator.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator is required to restrict all remote connections to use Institute resources and only allow the connections which obtains prior approval.

Control Number	Control Name	Priority
SC-7	Process Isolation	P1

Statement

The Higher Education Institutions are required to maintain their separate execution domain for each process.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network administrator shall maintain separate domain for each execution process.

Authority: [79] [80] [81] [82] [83] [15] [16] [97] [132] [124] [8] [11] [133] [90]–[94] [95] [24] [6] [20] [23]

6.2.23 System and Information Integrity

The system and information integrity module of the framework is developed to document the flaw remediation, rating of the vulnerabilities, threats, risks and remediation, protection against malicious code, continues monitoring of the information system of the institute, utilization of automatic tools for analysis of the flaws, risks, vulnerabilities and threats, generation of security alerts and directives, integrity of the software and firmware, protection of the system against spam, input and output validation, error handling and memory protection. The goals of this

modules are to maintain the integrity of the information system of the Institute by applying aforementioned techniques and tools.

6.5.23.1 System and Information Integrity Controls

Control Number	Control Name	Priority
SI-1	System and Information Integrity Policy and Procedures	P1

Statement

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of system and information integrity policy, roles and responsibilities of personnel, management commitment, define coordination among departments of the Institute, and compliance; procedures to implement of system and information integrity policy and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete the system and information integrity policy.

Control Number	Control Name	Priority
SI-2	Flaw Remediation	P1

Statement

The Higher Education Institutions shall identify flaws of the information system, reports, and take corrective measures to rectify flaws. The Network Administrator shall install all security related software updates like patches and service packs. All types of updates especially related to security are required to be tested for effectiveness before installation. The Network Administrator also shall handle

discovered flaws, continue monitoring, activities related to incident response which are required to be addressed immediately. The flaw remediation should be the part of configuration management process. The flaw remediation process is also required to be tracked and verified.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator shall implement planned flaw remediation procedures to handle with issues related to testing and implementation of security related software and firmware in the Institution. The configuration management policies described in this document must be adhered while dealing with remediation flaws.

Control Number	Control Name	Priority
SI-3	Malicious Code Protection	P1

Statement

The Higher Education Institute shall implement malicious code protection tools and techniques at the entry and exit point of the information system to detect and eliminate said codes. The Network Administrator shall keep update malicious code protection techniques as and when new release is available according to configuration management policy of the Institute. Periodic scans is required to be configured to scan malicious code in the information system. The Information System should be configured in a manner to take automatic auction against malicious code as found in the system.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☐ Physical ☐ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator shall implement malicious code detection, automatic eradicate, updates, review and scanning mechanism mechanisms in the Information System of the Institute.

Control Number	Control Name	Priority
SI-4	Information System Monitoring	P1

Statement

The Network Administrator shall plan and implement vulnerabilities, events, attacks, threats and indicators of potential attack's monitoring and reporting tools and techniques in the Information System to cater unauthorized access and to achieve monitoring objectives. Local, network and remote connections are also be required to be monitored. The Network Administrator shall also make sure that the monitoring information reported through the tools must retain confidential and protected from unauthorized access.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☐ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator shall utilize various tools and techniques to monitor all possible security issues. He will make sure that monitoring reports are secured and retained, test monitoring tools before implementing and document monitoring activities.

Control Number	Control Name	Priority
SI-5	Security Alerts, Advisories, and Directives	P1

Statement

The Network Administrator shall make sure that it will receive security alerts, advisories and directives on regular basis, transfer these alerts, advisories to the concerned personnel and take appropriate and relevant action as desired. The Head of the Institute shall notify the concerned personnel who shall act on these alerts and advisories.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Network Administrator shall receive security notices, alerts and advisories from the Higher Education and other Higher Education Institutions, utilize different tools to issue alert to the concerned personnel, and prepare weekly/monthly reports of compliance.

Control Number	Control Name	Priority
SI-12	Information Handling and Retention	P2

Statement

The Higher Education and its Institutions shall handle and retain information related to security of information system and information. The Higher Education shall develop record retention standard / policies and procedures.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control.

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance **Cloud Service Delivery Model**

☒ Physical ☒ Network ☒ Compute ☒ SaaS ☒ PaaS ☒ IaaS
☒ Storage ☒ Application ☒ Data

Implementation

The Head of the Institute or Network Administrator shall retain all information of the Information System and its output according to applicable policies and procedures of the Higher Education.

Authority: [79] [80] [81] [82] [83] [86] [93] [94] [97] [128] [30] [134]

6.2.24 System and Services Acquisition

The confidentiality, integrity and availability of the stored data of the Institute information system can be increased by designing, updating, implementing, testing, reviewing, and documenting the information security controls. This is the case irrespective of whether the Institute information system has been developed and maintained through internal Institute resources, acquired from Higher Education or through external service providers, or through an arrangement of internal and external information system resources. Whether information systems are developed or purchased, the identification of information security requirements at the beginning of SDLC is necessary to enhance the security of the Institute information systems and remove the practice of increasing security controls after the design of the information system.

The System and Service Acquisition discusses about allocation of resources, SDLC, acquisition process, documentation of the information system, principles of security engineering, services of the external services, hiring of system developers, external services, security testing and evaluation, Service Level Agreement, Service documentation and configuration management.

6.5.24.2 System and Services Acquisition Controls

Control Number	Control Name	Priority
SA-1	System and Services Acquisition Policy and Procedures	P1

Statement

Information system and services acquisition controls shall make sure that security of the Information System is adequately planned for the environment where IT assets are being evaluated.

The Higher Education shall develop, circulate, adhere, reviews existing formal policy and document and update information security system and services acquisition of the information system that addresses purpose, define the scope of System and Services Acquisition, roles and responsibilities of personnel, management commitment, define

coordination among departments of the Institute, and compliance; procedures to implement System and Services Acquisition and its associated controls.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☒ Faculty Member ☒ Student ☒ Staff Member ☒ Third Party / CSP
☒ Assets / Resources ☒ Visitors

Cloud Architectural Relevance

☒ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall establish, document, circulate, review and update the regulations and procedures at least annually or upon changes required, that shall be used to complete System and Services Acquisition.

Control Number	Control Name	Priority
SA-2	Allocation of Resources	P1

Statement

The Higher Education Institutions shall define information security needs for the information system and its service in mission critical process planning, document, and immediately required allocates resources to safeguard the systems and its service. The Head of the Institute or Network Administrator shall ensure that all security capabilities either hardware or software are procured. The Network Administrator shall make sure that all types of security tools are properly assessed, procurements of the all IT assets are made in secure manner and also securely became part of the Information System.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☒ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☒ Storage ☐ Application ☐ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education shall be responsible to arrange budget and Head of the Institute as well as Network Administrator is responsible for capital planning for IT assets to allocate proper resources for security. The Network Administrator shall submit request to the Head of the Institute for onward submission to the Higher Education authorities for the new IT assets and services on the basis of risk management.

Control Number	Control Name	Priority
SA-3	System Development Life Cycle	P1

Statement

The Higher Education is required to opt System Development Life Cycle (SDLC) plan for the development of all types of software in-house. During SDLC, risk management, threat management, vulnerabilities management, risk identification and mitigation shall be included in this process to make application more secure. It is also required that software must be documented and tested in the context of information security before implementing in Information System.

Notwithstanding of framework adopted, the following points are required to be addressed:

1. All Information Security related roles and responsibilities are required to be defined and properly documented.
2. The security responsibilities at individual level are required to be identified.
3. Appropriate and relevant Security controls are required to be applied on the stored or processed data by the application.
4. Risk Management must be integral part of the SDLC.
5. Relevant personnel are required to document each actively of the development and that documentation is maintained.
6. Along-with risk assessment, security testing and audit controls also shall be the part of system development life cycle to get the desired output and to meet the security requirements of the system.
7. The Head of the Institute or at-least Network Administrator shall approve and document that the developed information system is fully operational and secured.

8. Security reviews of the Information System is required to be conducted as and when modification and update is required in the system.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☒ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☐ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☐ Network ☐ Compute
☐ Storage ☐ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Network Administrator shall manage information system through system development life cycle and incorporating information security considerations, clearly define and document information security role and responsibility of personnel through SDLC and also define security role and responsibility of each individual.

Control Number	Control Name	Priority
SA-4	External Information System Services	P1

Statement

The Higher Education Institutions must ask to all external services providers to adhere with the Higher Education information security requirements and employ suitable security controls according to the requirement.

Applicability

This control applies to the selected titles and shall be responsible to adhere the Information Security Policies and Procedures mentioned in the control

☐ Higher Education ☒ ISO ☒ HOI / Custodian ☒ Network Admn.
☐ Faculty Member ☐ Student ☐ Staff Member ☒ Third Party / CSP
☐ Assets / Resources ☐ Visitors

Cloud Architectural Relevance

☐ Physical ☒ Network ☒ Compute
☒ Storage ☒ Application ☒ Data

Cloud Service Delivery Model

☒ SaaS ☒ PaaS ☒ IaaS

Implementation

The Higher Education Institutions are required to make sure that the external service providers meet the security requirements. Risks related to the external service providers are required to be taken into consideration while developing trust relationship. The trust relationship is required to be documented to monitor it time to time. A service level agreement must be signed among both the parties by defining

roles and responsibilities of individuals, expected performance of security controls, define measureable outcome, response time, remedies in the case of noncompliance.

Authority: [79][80][81][82][83] [15] [16] [97] [132] [124] [8] [11] [133] [90]–[94] [95] [24] [6] [20] [23]

6.3 RELIABILITY OF THE PROPOSED FRAMEWORK

The reliability of the system satisfy the four principles:

- Confidentiality
- Privacy
- Processing Integrity
- Availability

The proposed framework has 175 controls that satisfy these Principles. The 175 controls are basically classified into four principles.

Confidentiality Controls: Confidentiality checks ensure that private information is secure from prying eyes and is available only to authorized persons. It stops attackers to get their goals of divulging confidential information to unauthorized persons. Confidentiality controls include cryptographic controls, media access controls and access control lists etc.

Privacy Control: are designed to protect user's right to safeguarding its information from any other user/third party. It involves the protection of user's data and information not to disclose to other users and third parties. In general, privacy is the user's right to keep its data to itself. The proposed framework has controls that restrain unauthorized users to get access, review, correct and review user's data & information, disclosure of information to third parties, security to protect loss, quality to maintain integrity of the data / information, continuous monitoring of user's data and third parties to not use user's data or information.

Processing Integrity Controls: are developed to manage data integrity, which is a primary domain of the information security. Data integrity refers to the precision and consistency of information stored in a database, datacentre, data mart or other construct. Integrity controls are essential part of information security framework and helps to strengthen the organization's information integrity goals. These controls can be used to prevent user semantic errors, to defend against unauthorized modification

in the code of the software, to support prevent vulnerabilities and stop malicious code. Integrity controls apply rules that verify application and database operations are smooth, make sure that data is not corrupted by applying integrity control functions that are informed by business processes, computerized editions, and other types of security infrastructure.

Availability controls: are designed to make sure that web sited hosted on cloud computing, servers, clients are available 24/7 to authorized users. If an attacker attacks part of the IT infrastructure or a piece of hardware does not work, the availability checks help the organization to keep continue normal operations. Few types of such controls are relates to system availability control, data availability control viz-a-viz website availability controls. Availability failures can occur for various reasons, such as malicious users attempting to disable a website; or hardware failures such as hard disk or power supply failures; or errors in the code an application can download. They can also include utilities such as power outages that interrupt systems and networks.

The proposed framework outlines the baseline information security controls compulsory to equally protect the confidentiality, integrity, privacy and availability of information entrusted Higher Education Institutions in Table 6.

Table 6. Security Dimensions Corresponding to Control

Control No and Name		Conf.	Priv.	Integ.	Avail.
Access Control Family Controls					
AC-01	Access Control Policy and Procedures	✓	✓	✓	✓
AC-02	Account Management	✓		✓	
AC-03	Access Enforcement	✓	✓	✓	
AC-04	Information Flow Enforcement	✓			
AC-05	Separation of Duties	✓		✓	
AC-06	Least Privilege	✓	✓		
AC-07	Unsuccessful Login Attempts	✓	✓		
AC-08	System Use Notification	✓			
AC-09	Session Lock	✓			
AC-10	Permitted Actions without Identification or Authentication		✓		
AC-11	Remote Access	✓		✓	
AC-12	Wireless Access	✓	✓	✓	✓
AC-13	Access Control for Mobile Devices	✓		✓	
AC-14	User of External Information Systems	✓	✓	✓	
AC-15	Publicly Accessible Content	✓	✓		✓
Awareness and Training Family Controls					
AT-01	Security Awareness and Training Policy and Procedures	✓		✓	✓
AT-02	Awareness and Training Controls	✓			
AT-03	Role Based Security Training	✓	✓		
AT-04	Security Training Records	✓			
Audit and Accountability Family Controls					
AU-01	Audit & Accountability Controls	✓	✓	✓	✓
AU-02	Audit Events	✓	✓	✓	

Control No and Name		Conf.	Priv.	Integ.	Avail.
AU-03	Content of Audit Records	✓		✓	
AU-04	Audit Storage Capacity	✓		✓	✓
AU-05	Response to Audit Processing Failures	✓		✓	
AU-06	Audit Review, Analysis, and Reporting	✓	✓	✓	✓
AU-07	Time Stamps			✓	
AU-08	Protection of Audit Information	✓	✓	✓	
AU-09	Audit Record Retention			✓	✓
AU-10	Audit Generation	✓		✓	
Configuration Management Family Controls					
CM-01	Configuration Management Controls	✓		✓	✓
CM-02	Baseline Configuration	✓		✓	
CM-03	Security Impact Analysis	✓		✓	
CM-04	Least Functionality		✓	✓	✓
CM-05	Information System Component Inventory	✓		✓	
CM-06	Software Usage Restrictions	✓	✓	✓	✓
CM-07	User Installed Software	✓		✓	
Contingency Planning Family Controls					
CP-01	Contingency Planning Controls	✓		✓	✓
CP-02	Contingency Plan			✓	✓
CP-03	Contingency Training	✓			✓
CP-04	Contingency Plan Testing			✓	✓
CP-05	Information System Backup	✓	✓	✓	✓
CP-06	Information System Recovery and Reconstitution		✓	✓	✓
Maintenance Family Controls					
MA-01	System Maintenance Policy and Procedures	✓		✓	✓
MA-02	Controlled Maintenance		✓	✓	✓
MA-03	Non-local Maintenance	✓		✓	
MA-04	Maintenance Personnel			✓	✓
Media Protection Family Controls					
MP-01	Media Protection Policy and Procedures	✓	✓		✓
MP-02	Media Access	✓	✓	✓	
MP-03	Media Sanitization	✓	✓	✓	
MP-04	Media Use	✓	✓	✓	✓
Planning Family Controls					
PL-01	Security Planning Policy and Procedures	✓		✓	✓
PL-02	System Security Plan	✓	✓	✓	✓
PL-03	Rules of Behavior	✓	✓		
Risk Assessment Family Controls					
RA-01	Risk Assessment Policy and Procedures	✓	✓	✓	✓
RA-02	Security Categorization	✓	✓	✓	✓
RA-03	Risk Assessment	✓	✓	✓	
RA-04	Vulnerability Scanning	✓	✓	✓	
System and Services Acquisition Family Controls					
SA-01	System and Services Acquisition Policy and Procedures	✓		✓	✓
SA-02	Allocation of Resources				✓
SA-03	System Development Life Cycle		✓	✓	✓
SA-04	External Information System Services	✓		✓	✓
Identification and Authentication Family Controls					
IA-01	Identification and Authentication Policy and Procedures	✓	✓	✓	✓
IA-02	Identification and Authentication (Organizational Users)	✓		✓	
IA-03	Identifier Management	✓		✓	
IA-04	Authenticator Management	✓		✓	
IA-05	Authenticator Feedback	✓			
IA-06	Cryptographic Module Authentication	✓	✓	✓	
IA-07	Identification and Authentication (Non-Institutional Users)	✓	✓	✓	
Incident Response Family Controls					
IR-01	Incident Response Policy and Procedures	✓		✓	✓
IR-02	Incident Response Training				✓
IR-03	Incident Handling		✓	✓	✓
IR-04	Incident Monitoring	✓	✓		✓

Control No and Name		Conf.	Priv.	Integ.	Avail.
IR-05	Incident Response Assistance				✓
IR-06	Incident Response Plan	✓			✓
Personnel Security Family Controls					
PS-01	Personnel Security Policy and Procedures	✓	✓	✓	✓
PS-02	Position Risk Designation	✓	✓		✓
PS-03	Personnel Screening	✓	✓		
PS-04	Personnel Termination	✓	✓	✓	
PS-05	Personnel Transfer	✓	✓		✓
PS-06	Access Agreements	✓	✓		
PS-07	Third-Party Personnel Security	✓	✓	✓	
PS-08	Personnel Sanctions	✓	✓		✓
System and Information Integrity Family Controls					
SI-01	System and Information Integrity Policy and Procedures	✓		✓	✓
SI-02	Flaw Remediation			✓	✓
SI-03	Malicious Code Protection	✓	✓	✓	
SI-04	Information System Monitoring	✓		✓	
SI-05	Security Alerts, Advisories, and Directives	✓		✓	
Physical and Environmental Protection Family Controls					
PE-01	Physical and Environmental Protection Policy and Procedures	✓		✓	✓
PE-02	Physical Access Authorizations	✓	✓	✓	✓
PE-03	Physical Access Control	✓	✓	✓	✓
PE-04	Monitoring Physical Access	✓		✓	✓
PE-05	Visitor Access Records	✓		✓	✓
PE-06	Emergency Lighting				✓
PE-07	Fire Protection				✓
PE-08	Temperature and Humidity Controls				✓
PE-09	Water Damage Protection				✓
PE-10	Delivery and Removal			✓	✓
Program Management Family Controls					
PM-01	Program Management Policy and Procedures	✓		✓	✓
PM-02	Information Security Officer			✓	
PM-03	Information Security Resources				✓
PM-04	Plan of Action and Milestones Processes	✓		✓	
PM-05	Information System Inventory	✓		✓	
PM-06	Information Security Measures of Performance	✓		✓	✓
PM-07	Enterprise Architecture			✓	
PM-08	Threat Awareness Program	✓		✓	
Security Assessment and Authorization Family Controls					
CA-01	Security Assessment and Authorization Policies and Procedures	✓		✓	✓
CA-02	Security Assessments	✓	✓	✓	✓
CA-03	Information System Connections	✓	✓		
CA-04	Plan of Action and Milestones		✓	✓	
CA-05	Security Authorization	✓	✓		
CA-06	Continuous Monitoring	✓	✓		✓
CA-07	Internal System Connections	✓	✓		
System and Communications Protection Family Controls					
SC-01	System and Communications Protection Policy and Procedures	✓	✓	✓	✓
SC-02	Denial of Service Protection				✓
SC-03	Boundary Protection		✓	✓	✓
SC-04	Cryptographic Key Establishment and Management	✓	✓	✓	
SC-05	Cryptographic Protection	✓	✓		
SC-06	Collaborative Computing Devices	✓	✓		✓
SC-07	Process Isolation	✓	✓		✓
Mobile Security Family Controls					
MS-01	Mobile Security Policy and Procedure	✓	✓	✓	✓
MS-02	Anti-Malware	✓	✓		
MS-03	Application Stores	✓	✓	✓	
MS-04	Approved Applications and Stores	✓	✓	✓	
MS-05	Approved Software for BYOD		✓	✓	

Control No and Name		Conf.	Priv.	Integ.	Avail.
MS-06	Mobile Awareness and Training		✓		✓
MS-07	Cloud Based Services				✓
MS-08	Compatibility			✓	✓
MS-09	Device Eligibility		✓	✓	
MS-10	Device Inventory	✓		✓	✓
MS-11	Device Management			✓	
MS-12	Encryption	✓	✓	✓	
MS-13	Jailbreaking and Rooting			✓	
MS-14	Lockout Screen	✓			
MS-15	Passwords	✓	✓	✓	
MS-16	Backup Policy		✓	✓	✓
MS-17	Security Patches	✓	✓	✓	
Infrastructure & Virtualization Security Family Controls					
IV-01	Infrastructure & Virtualization Security Policy and Procedure	✓		✓	✓
IV-02	Audit Logging / Intrusion Detection	✓	✓	✓	
IV-03	Change Detection			✓	
IV-04	Clock Synchronization			✓	
IV-05	Information System Documentation			✓	
IV-06	Vulnerability Management	✓		✓	✓
IV-07	Network Security	✓		✓	✓
IV-08	OS Hardening and Base Controls	✓		✓	
IV-09	Separation of Environment	✓		✓	
IV-10	Segmentation	✓		✓	✓
IV-11	VM Security - Data Protection	✓		✓	
IV-12	Hypervisor Hardening	✓		✓	
IV-13	Network Architecture			✓	✓
Interoperability & Portability Family Controls					
IP-01	Interoperability & Portability	✓		✓	✓
IP-02	APIs				✓
IP-03	Data Request			✓	✓
IP-04	Standardized Network Protocols			✓	✓
IP-05	Virtualization	✓			✓
Business Continuity Management & Operational Resilience Family Controls					
BC-01	Business Continuity Management & Operational Reliance	✓		✓	✓
BC-02	Business Continuity Planning				✓
BC-03	Business Continuity Testing				✓
BC-04	Datacenter Utilities / Environmental Conditions			✓	✓
BC-05	Equipment Location and Maintenance			✓	✓
BC-06	Impact Analysis		✓		✓
BC-07	Retention Policy	✓			✓
Data Security & Information Life-Cycle Management Family Controls					
DS-01	Data Security & Information Life-Cycle Management Policy & Procedures	✓		✓	✓
DS-02	Classification	✓		✓	✓
DS-03	Ecommerce Transactions	✓		✓	
DS-04	Handling / Labeling / Security Policy	✓		✓	✓
DS-05	Ownership / Stewardship	✓		✓	
Supply Chain Management, Transparency, and Accountability Family Controls					
SM-01	Data Quality and Integrity	✓		✓	✓
SM-02	Incident Reporting				✓
SM-03	Network and Infrastructure Services		✓	✓	✓
SM-04	Institute Internal Assessments		✓		✓
SM-05	Supply Chain Agreements				✓
SM-06	Supply Chain Governance Reviews	✓		✓	✓
SM-07	Third Party Assessment		✓		✓
SM-08	Third Party Audits		✓	✓	✓

6.4 COMPARISON OF THE PROPOSED FRAMEWORK WITH OTHER RENEWED INFORMATION SECURITY FRAMEWORKS

During literature review, the author studied different stereo-type criteria to compare more than two information security frameworks. Mostly Security frameworks which uses only security related techniques as benchmark and overlook the Cloud Computing related features. During literature review, the author could not find any specific criteria in which cloud computing information security framework for higher education Institutions was compared with other information security framework. The authors studied four renowned Information Security frameworks thoroughly and wrote their common and distinguished assessment points to formulate a comprehensive criteria for the evaluations of existing Information Security Framework with the proposed cloud computing based information security framework for higher education. The authors critically analyzed each of the task covered under study frameworks, collected the relevant characteristics from other information security frameworks and thereafter, combined them to formulate one task that covers all approaches opted by other frameworks. The said approach is very comprehensive as the developed characteristics are taken from surveyed information security frameworks. Furthermore, during literature review, the Educause in August, 2018 has developed "*Information Security Program Assessment Tool*" with the support of Higher Edu. Info. Security Council, Community to evaluate the maturity of security programs of the Higher Education Institution. In the said assessment tools, 101 characteristics of the information security framework were designed by covering 12 broad areas. The author initially selected characteristics from said assessment tool and also added further characteristics in this comparison Table 8 like mobile cloud computing, virtualization and etc.

The author also developed a simple criteria to quantify each renowned information security framework and the same has been implemented on proposed the proposed framework of this thesis to show its better effectiveness.

The criteria developed for comparison is given in Table 7. Each framework and its associated characteristics will be selected and passed through criteria to get the results.

Table 7. Information Security Frameworks Comparison Criteria

Value	Description	Remarks
0	No Characteristics	The framework does not support the

Value	Description	Remarks
		characteristic of the IS framework
1	Slightly Characteristics	The framework has controls that meet slightly characteristics
2	Somewhat Characteristics	The framework controls meet somewhat characteristics of the IS framework
3	Complete Characteristics	The IS Framework has one or more than one controls that completely support the characteristic

The developed criteria implemented on four renowned information security frameworks and their scores compared with the proposed framework of this thesis to validate its reliability and effectiveness. The given Table 8 is showing the comparison.

Table 8: Comparison of Proposed Information Security Frameworks with Renowned Frameworks

Sr. No	Characteristics	SHCF	CCM	NIST	ISO	COBIT
1	**Human Resource Security**					
1	Information security awareness training	3	3	3	3	2
2	Specialized role-based training	3	2	3	3	2
3	Clearly state responsibilities, liabilities, and consequences	3	2	2	1	1
4	Rescinding system and building access on assets and return assigned assets to users	3	2	3	2	1
5	When position or responsibility change, revoking system access to users	3	2	3	2	3
	Sub Total	**15**	**11**	**14**	**11**	**9**
2	**Asset Management**					
6	Critical information about the assets and the functions	3	3	3	3	3
7	Classify information to indicate that the appropriate levels of information security in the Institute	3	3	3	3	3
	Sub Total	**6**	**6**	**6**	**6**	**6**
3	**Access Control**					
8	Access control policy for authorizing the Institute and non-institute users	3	3	3	3	2
9	Revoking access rights to information systems in the event of change in information system	3	2	3	3	2
10	Granting and revoking appropriate user access to information system	3	2	3	3	2
11	Strong password management program in the Institute	3	3	3	3	3
12	Review users' access to information system to ensure only needed privileges are applied	3	3	3	3	1
13	Measures to secure remote access services of the Institute	3	3	3	3	3
14	Restrict Institute's unencrypted sensitive information to the external untrusted networks	3	2	2	2	3
15	Manage Institute's digital identities throughout their life cycle, from registration through termination	3	2	3	1	3
16	Restrict the sharing of passwords to Institute users and visitors	3	3	3	3	3
17	Prohibit the Institute users to not use of generic type of accounts with privileged access to systems	3	2	3	3	3
18	Application of higher levels of authentication in the Institute to protect the Institute's resources with higher levels of sensitivity	3	3	2	1	1
19	Applying of time limits lockout on login failure	3	3	3	3	3
20	Isolating Institute's sensitive data, proper procedures to protect Institute's data from unauthorized access	3	3	2	2	2

Sr. No	Characteristics	SHCF	CCM	NIST	ISO	COBIT
	and eavesdropping					
21	Multifactor access policy in the Institute and security requirements for the end point	3	3	2	2	1
	Sub Total	**42**	**37**	**38**	**35**	**32**
4	**Cryptography**					
22	Appropriate/vetted Institute's encryption methods to protect sensitive data of the Institute in transit	3	3	3	3	2
23	Policies regarding the use encryption on the information stored in the media, transit, the Institute's sensitive and on the confidential information of the users.	3	3	3	3	2
24	Documentation regarding Key management and it's employed	3	3	3	3	2
	Sub Total	**9**	**9**	**9**	**9**	**6**
5	**Physical and Environmental Security**					
25	Only authorized users of the Institute are allowed physical access to information system and its resources	3	3	3	3	3
26	Protect critical hardware of the Institute and wiring of the network from natural and man-made security threats	3	2	3	2	3
27	Proper and secure issuance of the secure area keys, codes, and cards that used for appropriate authorization	3	3	2	3	2
28	Adherence with Institute's approved vendor-recommended guidance to maintain equipment and services	3	2	1	1	1
29	Proper media sanitization before final disposal, reuse and release to users	3	3	3	3	3
30	Appropriate detection mechanism of unauthorized removal of Institute's equipment, information and software	3	3	2	3	3
31	Emergency Lighting arrangements, Fire Protection system, Temperature and Humidity system and Water Damage Protection available in the Datacenter of the Institute	3	3	3	1	1
	Sub Total	**21**	**19**	**17**	**16**	**16**
6	**Operations Security**					
32	Maintain security configuration standards in the Institute for information systems and its applications	3	2	2	2	2
33	Changes in the tested information systems, authorized and reported to users	3	2	2	2	2
34	Segregation of personnel duties to make sure unplanned or unauthorized modification of information	3	2	3	2	2
35	The production systems of the Institute should be separate from other stages of the SDLC	3	2	2	3	1
36	Utilization of the main system resources to reduce the risk and monitoring these activities	3	3	2	2	1
37	Detection of malicious codes inside software, e-mails, websites and removable media of the Institute	3	2	2	1	2
38	Backup policy is implemented and consistent to meet the Institute's requirements.	3	3	2	3	3
39	Virus detection through antivirus, installation of firewall, installation of patches before the connectivity of the resources to internet	3	3	2	2	2
40	The network of the Institute is segmented to implement multi-level security on the basis of classification of information	3	3	3	2	2
41	The Internet accessible servers of the Institute are protected through multi-level security layer	3	2	1	2	2
42	All types of the Institute's media that are used in secure sites of the Institute should be protected, tracked, and its reporting mechanism developed	3	2	3	3	1
43	Data related to e-commerce traversing through public	3	3	3	2	2

Sr. No	Characteristics	SHCF	CCM	NIST	ISO	COBIT
	networks is shielded from fraudulent activities and its integrity maintained					
44	Automatic audit logging of the Institute's assets configuration changes, privilege assignments, access attempts, and authorization	3	2	2	2	1
45	Continuous monitoring of audit logs to detect unauthorized access and anomalous activities	3	2	2	2	3
46	Only authorized personnel are allowed to view logs	3	2	3	3	3
47	Audit log data secure from unauthorized access and tampering	3	3	3	3	3
48	Rights to review audit logs regularly reviewed	3	2	3	3	2
49	File integrity monitoring tools are required to alert users about unauthorized changes in their files	3	2	2	3	3
50	The clocks of the all network computers synchronized with all clocks of the networks	3	2	3	2	3
	Sub Total	**57**	**44**	**45**	**44**	**40**
7	**Communications Security**					
51	Agreement between Institute and its users and third parties regarding confidentiality and nondisclosure of information	3	2	1	2	1
52	Testing of restore procedures	3	2	1	2	1
53	Continuously monitoring of wired and wireless networks of the Institute against unauthorized access	3	3	3	3	3
54	Protection of information transit between Institute users and third parties against copying, modification, destruction and interception	3	2	2	2	3
55	Configuration ports and diagnostic tool are protected from unauthorized access and malicious software	3	2	3	3	3
56	Prevention measures against fake/rogue wireless access points working within institute boundary	3	2	3		3
	Sub Total	**18**	**13**	**13**	**12**	**14**
8	**Systems Acquisition, Development, and Maintenance**					
57	Validation about the security of the purchased application and system software products and services for the Institute	3	2	2	3	3
58	Validation of new recommended changes before its installation in the system	3	3	2	3	2
59	Protect coding practices and consider security vulnerabilities in common applications.	2	3	1	3	1
60	Detection of corruption in software applications of the Institute and validation checks	3	2	2	3	1
61	Checks to make sure Message integrity	3	3	3	3	3
62	Substantiation checks to make sure data output is as predictable	3	2	3	2	3
63	Maintain the source code of critical applications during the development life cycle to correct errors after testing the Institute application	2	3	3	2	2
64	Safety rules for sensitive test data applied to sensitive production data	2	2	3	2	2
65	Restrict and monitor access to source code libraries to reduce the risk of corruption	3	3	3	2	2
66	Modifications to critical systems are valid for commercial reasons and have received the appropriate authorization	3	3	3	3	1
67	Changes made in the production systems of the Institute do not have a negative impact on safety or operations	3	2	2	2	2
68	Tools, techniques and procedures to monitor and prevent the loss of confidential data	3	2	2	1	2
69	The contractual agreements include security requirements for the development of outsourced software	3	3	3	1	1
70	Patch management strategies are properly functioning	3	3	3	2	2
71	Responsibilities assigned to monitor and respond quickly to patch reviews, security bulletins and	2	2	2	3	2

Sr. No	Characteristics	SHCF	CCM	NIST	ISO	COBIT
	vulnerability reports					
	Sub Total	**41**	**38**	**37**	**35**	**29**
9	**Supplier Relationships**					
72	Security requirements are included in the agreement with third parties before giving access to confidential institutional information resources	3	3	2	2	2
73	Requirements addressed and corrected before granting access to data, resources and information systems	2	2	2	3	2
74	Agreement with third parties have appropriate security requirements	2	1	2	2	1
75	Third parties comply with suitable information security desires	3	2	2	1	1
76	Third parties make sure the compliance with information security controls monitoring	3	3	2	1	1
77	Contracts of third-party services executed and reviewed to guarantee security requirements	3	3	3	2	2
	Sub Total	**16**	**14**	**13**	**11**	**9**
10	**Information Security Incident Management**					
78	Incident-handling policies and procedures are intact to report security events during incident handling	3	2	2	2	2
79	Incident response personnel awareness on legal or compliance requirements	2	1	1	2	2
	Sub Total	**5**	**3**	**3**	**4**	**4**
11	**Information Security Aspects of Business Continuity Management**					
80	Business Continuity Planning for Institutions	3	3	3	3	2
81	Business Continuity Testing at regular interval	3	3	3	1	1
82	Datacenter Utilities / Environmental Conditions are suitable	3	3	2	1	1
83	Equipment Location and Maintenance are properly secured	3	2	3	2	1
84	Impact Analysis of the business continuity	3	2	3	1	1
85	Retention Policies are intact	3	3	3	1	3
	Sub Total	**18**	**16**	**17**	**9**	**9**
12	**Compliance**					
86	Records management policies that addresses the life cycle of paper and electronic documents.	3	2	3	2	3
87	Applicable data protection policy covering personally identifiable information	3	2	2	3	2
88	Acceptable Use Policy (AUP) that inappropriate use	3	1	2	2	2
89	Community guide on export control laws	2	2	1	2	2
90	All SOPs are periodically evaluated to comply with the Institute's policies, standards and safety procedures	3	3	3	1	3
91	Run vulnerability tests at the application level and network level	3	3	3	2	2
92	Independent audits of the Institute’s information systems to identify strengths and weaknesses of the system	3	3	3	3	3
93	Control tools have been properly separated from the development and operation environments of the system to avoid any misuse or compromise	3	3	3	3	3
	Sub Total	**23**	**19**	**20**	**18**	**20**
13	**Mobile Security**					
94	Mobile computing usage guideline for users to store, process, or transmit user and institutional data	3	2	2	1	2
95	Encryption on mobile computing devices	3	2	2	2	2
96	Detect, quarantine, and eradicate known malicious code on information systems including workstations, servers, and mobile computing devices	3	1	2	1	1
97	Approved Applications and Stores	3	3	2	1	1
98	Approved Software for BYOD	3	3	1	1	1
99	Cloud Based Services	3	3	1	1	1
100	Compatibility of the applications with other applications	3	3	1	0	1
101	Device Eligibility defined to allow only authorized	3	3	2	1	1

Sr. No	Characteristics	SHCF	CCM	NIST	ISO	COBIT
	devices					
102	Device Inventory maintained in the institute	3	3	2	1	1
103	Device Management is properly configured	3	3	1	1	1
104	Jailbreaking and Rooting	3	3	1	0	0
105	Critical mobile Apps are Password protected	3	3	0	1	1
106	Mobile Backup on another storage media and remote site	3	2	1	0	0
107	Security Patches installed on the mobile device	3	3	0	0	0
	Sub Total	**42**	**37**	**18**	**11**	**13**
14	**Interoperability & Portability**					
108	Third party use Standard APIs	3	3	2	0	0
109	Third party provide Data on Request	3	3	2	1	1
110	Third party use Standardized Network Protocols	3	3	1	1	2
111	Virtualization	3	2	1	1	2
	Sub Total	**12**	**11**	**6**	**3**	**5**
15	**Identification and Authentication**					
112	Identification and Authentication (Institutional Users)	3	3	3	3	3
113	Identifier Management	3	3	2	2	3
114	Authenticator Management	3	2	1	3	3
115	Authenticator Feedback	3	3	1	1	2
116	Cryptographic Module Authentication	3	3	2	1	3
117	Identification and Authentication (Non-Institutional Users)	3	3	2	3	2
	Sub Total	**18**	**17**	**11**	**13**	**16**
16	**Infrastructure & Virtualization Security**					
118	Audit Logging / Intrusion Detection	3	3	3	3	3
119	Information System Documentation	3	2	3	3	3
120	OS Hardening and Base Controls	3	3	2	1	1
121	Separation of Environment	3	3	2	0	1
122	VM Security - Data Protection	3	3	3	1	1
123	Hypervisor Hardening	3	2	2	0	1
	Sub Total	**18**	**16**	**15**	**8**	**10**
17	**System and Services Acquisition**					
124	Allocation of Resources	3	3	2	2	2
125	System Development Life Cycle	3	2	3	3	2
126	External Information System Services	3	3	2	3	3
	Sub Total	**9**	**8**	**7**	**8**	**7**
18	**System and Information Integrity**					
127	Flaw Remediation	3	2	3	2	2
128	Provider Internal Assessments	3	3	3	3	3
129	Supply Chain Agreements	3	3	3	3	3
130	Supply Chain Governance Reviews	3	3	3	3	3
131	Third Party Assessment	3	3	2	1	2
132	Third Party Audits	3	3	2	1	1
	Sub Total	**18**	**17**	**16**	**13**	**14**
	Grand Total	**388**	**335**	**305**	**266**	**259**

After summing the score of 132 characteristics vertically, the results show that the proposed framework has obtained highest score whereas on the other hand, the Cloud Control Matrix V3.0.1is the second in rating.

The NIST SP 800-53 Rev.4, ISO/IEC 27001:2013 and COBIT 5.0 on third, fourth and fifth position in rating. The results of Cloud Control Matrix V3.0.1 clearly states that it is a comprehensive method and Industry recommends it.

Although NIST SP 800-53 Rev.4 A has many citations, a number of researchers used this method in their research but results revealed that this framework still needs

improvement in the context of cloud computing and third parties controls. The results of COBIT 5.0 are not unexpected, during its study, noticed its effectiveness and loopholes.

It is also noticed that ISO/IEC 27001:2013 is immature information security framework to deal with cloud computing, mobile security, virtualization security, third parties security issues, and infrastructure security and it was built to cater the needs of specific traditional IT areas not to cover all Information Security issues especially in the context to cloud computing. It is concluded in comparison to inform the readers about which areas of the renowned information security frameworks are still need improvement.

6.5 EFFECTIVENESS OF THE PROPOSED FRAMEWORK

The primary goals of the Information Security frameworks is to mitigate the information security risks and counter the information security threats and vulnerabilities. To check the effectiveness of the proposed framework, different techniques were studied and the found risk mapping is the most appropriate techniques among all other techniques. To do this task, first, the author identified cloud based information security risks and then these identified cloud security risks were mapped to the proposed framework to get know whether the proposed framework has adequate number of information security controls to mitigate the risks to give assurance to the Higher Education Institutions. The identification of the cloud based information security risks are given in the next section. To accomplish this task, the author select one identified risk and mapped in to all the proposed information security controls and domains to find out appropriate controls to mitigate the risks and similarly selected all the risks and mapped into appropriate information security controls. The research found that by implementing proposed framework and its information security controls, it provide complete assurance to the Higher Education Institutions to mitigate information security risks.

6.5.1 **Cloud Risk Identification**

This section of the dissertation deals with the identification of the risks that are relates to Cloud computing and the methods used to identity such types of risks. A systematic literature review was conducted to study the information security risks that have been identified by the researchers, academicians, industry, experts and organizations. In order to elicit only cloud security specific risks, it was decided to

select only the risks that cloud experts and cloud organizations reported. After applying said approach, a number of information security related risks were identified relates to different category of clouds. Thereafter, it was decided that the identified information security risks should be filtered to find out only cloud security related risks that Higher Education Institutions faced during and after the deployment of the cloud in their Institutions.

The list of the information security related risks was scrutinized to categorize the cloud security related risks. Thereafter, one more filter was applied to evaluate find out worthwhile risks and eliminate cosmetic risks. These finally identified risks are given in the given below Table 9. Although this list is not exhaustive one, but this list covers all types of the cloud security related risks.

Table 9. Mapping of Security Risks and Threats to proposed Information Security Controls

Sr. No	Risk and Threat's Description	Control Number and Description
1.	Data Breaches	AC-01: Access Control Policy and Procedures AC-04: Information Flow Enforcement AC-13: Access Control for Mobile Devices IA-02: Identification and Authentication IA-03: Identifier Management IA-05: Authenticator Feedback IA-06: Cryptographic Module Authentication IV-10: Segmentation IV-12: Hypervisor Hardening MP-03: Media Sanitization MS-12: Encryption PS-03: Personnel Screening RA-03: Risk Assessment RA-04: Vulnerability Scanning SC-01: System and Communications SC-04: Cryptographic Key Establishment and Management SC-05: Cryptographic Protection
2.	Insufficient Identity, Credential and Access Management	AC-03: Access Enforcement AT-02: Awareness and Training Controls AT-03: Role Based Security Training AU-08: Protection of Audit Information CM-04: Least Functionality IA-02: Identification and Authentication (Organizational Users) IA-03: Identifier Management IA-04: Authenticator Management IA-05: Authenticator Feedback IA-06: Cryptographic Module Authentication IA-07: Identification and Authentication (Non-Institutional Users) IV-08: OS Hardening and Base Controls PS-04: Personnel Termination PS-06: Access Agreements PS-08: Personnel Sanctions
3.	Insecure Interfaces and APIs	IA-02: Identification and Authentication (Organizational Users) IA-04: Authenticator Management IP-02: APIs PS-06: Access Agreements SM-03: Network / Infrastructure Services System and Communications Protection Family

Sr. No	Risk and Threat's Description	Control Number and Description
4.	System Vulnerabilities	CA-06: Continuous Monitoring IV-06: Vulnerability Management IV-08: OS Hardening and Base Controls RA-04: Vulnerability Scanning Risk Management Family System and Information Integrity Family
5.	Account Hijacking	AC-01: Access Control Policy and Procedures AC-03: Access Enforcement AC-05: Separation of Duties AC-06: Least Privilege AU-06: Audit Review, Analysis, and Reporting IA-01: Identification and Authentication Policy and Procedures IA-02: Identification and Authentication (Organizational Users) IA-03: Identifier Management IA-04: Authenticator Management IA-05: Authenticator Feedback IA-06: Cryptographic Module Authentication IA-07: Identification and Authentication (Non-Institutional Users) IR-03: Incident Handling PS-06: Access Agreements
6.	Malicious Insiders	AC-02: Account Management AC-05: Separation of Duties AC-06: Least Privilege AU-06: Audit Review, Analysis, and Reporting Incident Response Policies, Procedures and Principles IV-10: Segmentation MA-01: System Maintenance Policy and Procedures MA-01: System Maintenance Policy and Procedures MA-02: Controlled Maintenance PE-02: Physical Access Authorizations PE-03: Physical Access Control PE-04: Monitoring Physical Access Physical and Environmental Protection Policies, Procedures and Principles PS-02: Position Risk Designation PS-03: Personnel Screening PS-03: Personnel Screening PS-06: Access Agreements PS-08: Personnel Sanctions RA-03: Risk Assessment RA-04: Vulnerability Scanning SC-4: Cryptographic Key Establishment and Management SM-8: Third Party Audits System and Communications Protection Policies, Procedures and Principles System and Information Integrity Policies, Procedures and Principles
7.	Advanced Persistent Threats	AU-06: Audit Review, Analysis, and Reporting IV-03: Change Detection IV-05: Information System Documentation IV-06: Vulnerability Management IV-08: OS Hardening and Base Controls IV-13: Network Architecture SI-02: Flaw Remediation SI-03: Malicious Code Protection System and Communications Protection Policies, Procedures and Principles
8.	Data Loss	BC-04: Datacenter Utilities / Environmental Conditions BC-05: Equipment Location and Maintenance BC-07: Retention Policy RA-03: Risk Assessment
9.	Insufficient Due Diligence	AU-02: Audit Events AU-10: Audit Generation

Sr. No	Risk and Threat's Description	Control Number and Description
		BC-01: Business Continuity Management & Operational Reliance BC-02: Business Continuity Planning BC-03: Business Continuity Testing BC-04: Datacenter Utilities / Environmental Conditions BC-05: Equipment Location and Maintenance BC-06: Impact Analysis BC-07: Retention Policy IV-07: Network Security IV-10: Segmentation RA-01: Risk Assessment Policy and Procedures RA-02: Security Categorization RA-03: Risk Assessment RA-04: Vulnerability Scanning
10.	Abuse and Nefarious Use of Cloud Services	IR-01: Incident Response Policy and Procedures IR-02: Incident Response Training IR-03: Incident Handling IR-04: Incident Monitoring IR-05: Incident Response Assistance IR-06: Incident Response Plan PS-03: Personnel Screening PS-04: Personnel Termination PS-05: Personnel Transfer
11.	Denial of Service	IV-05: Information System Documentation Physical and Environmental Protection Family SA-02: Allocation of Resources SA-04: External Information System Services SC-02: Denial of Service Protection System and Communications Protection Family
12.	Shared Technology Vulnerabilities	IA-06: Cryptographic Module Authentication Incident Response Policies, Procedures and Principles IV-02: Audit Logging / Intrusion Detection IV-09: Separation of Environment IV-10: Segmentation MS-12: Encryption MS-17: Security Patches RA-03: Risk Assessment SC-05: Cryptographic Protection
13.	Loss of Governance	SM-07: Third Party Assessment SM-08: Third Party Audits Business Continuity Management & Operational Resilience Policies, Procedures and Principles Incident Response Policies, Procedures and Principles Interoperability & Portability Policies, Procedures and Principles Personnel Security Policies, Procedures and Principles
14.	Lock-in	Business Continuity Management & Operational Resilience Policies, Procedures and Principles Interoperability & Portability Policies, Procedures and Principles IP-01: Interoperability & Portability IP-02: APIs IP-03: Data Request IP-04: Standardized Network Protocols IP-05: Virtualization System and Services Acquisition Policies, Procedures and Principles
15.	Improper Backup	Audit and Accountability Policies, Procedures and Principles BC-7: Retention Policy Contingency planning Policies, Procedures and Principles CP-05: Information System Backup CP-06: Information System Recovery and Reconstitution MS-16: Backup Policy
16.	Third parties communication and service change risks	Access Control Policies, Procedures and Principles CA-03: Information System Connections Data Security & Information Life-Cycle Management

Sr. No	Risk and Threat's Description	Control Number and Description
		Policies, Procedures and Principles Infrastructure & Virtualization Policies, Procedures and Principles IV-03: Change Detection IV-04: Clock Synchronization Maintenance Policies, Procedures and Principles Mobile Security Policies, Procedures and Principles MS-02: Anti-Malware MS-15: Passwords Policies, Procedures and Principles PS-07: Third-Party Personnel Security SM-02: Incident Reporting SM-03: Network / Infrastructure Services SM-07: Third Party Assessment SM-08: Third Party Audits Supply Chain Management, Transparency and Accountability
17.	Unsafe working environment	BC-04: Datacenter Utilities / Environmental Conditions Contingency planning Policies, Procedures and Principles Infrastructure & Virtualization Policies, Procedures and Principles IV-09: Separation of Environment PE-01: Physical and Environmental Protection Policy and Procedures PE-02: Physical Access Authorizations PE-03: Physical Access Control PE-04: Monitoring Physical Access PE-05: Visitor Access Records PE-06: Emergency Lighting PE-07: Fire Protection PE-08: Temperature and Humidity Controls PE-09: Water Damage Protection PE-10: Delivery and Removal Physical and Environmental Protection Policies, Procedures and Principles
18.	Distributed Denial of Service	IV-05: Information System Documentation Physical and Environmental Protection Family SA-02: Allocation of Resources SA-04: External Information System Services SC-02: Denial of Service Protection System and Communications Protection Family
19.	Regularity Requirements	AU-09: Audit Record Retention BC-07: Retention Policy IV-02: Audit Logging / Intrusion Detection Supply Chain Management, Transparency and Accountability Policies, Procedures and Principles
20.	Service provider human error	Data Security & Information Life-Cycle Management PS-07: Third-Party Personnel Security SM-07: Third Party Assessment
21.	License risks	CM-07: User Installed Software CP-01 Configuration Management MA-02: Controlled Maintenance MP-03: Media Sanitization
22.	Loss of user account and configuration data	AC-01: Access Control Policy and Procedures AC-02: Account Management AC-04: Information Flow Enforcement AC-06: Least Privilege AC-10: Permitted Actions without Identification or Authentication AC-11: Remote Access AC-12: Wireless Access AC-13: Access Control for Mobile Devices AC-14: User of External Information Systems AC-15: Publicly Accessible Content Business Continuity Management & Operational Resilience Policies, Procedures and Principles
23.	Insecure or ineffective deletion of	Business Continuity Management & Operational Resilience

Sr. No	Risk and Threat's Description	Control Number and Description
	Institute data by the third party	Policies, Procedures and Principles SA-04: External Information System Services SM-05: Supply Chain Agreements SM-07: Third Party Assessment SM-08: Third Party Audits Supply Chain Management, Transparency and Accountability Policies, Procedures and Principles System and Services Acquisition Policies, Procedures and Principles
24.	Data interception	MS-12: Encryption Physical and Environmental Protection Policies, Procedures and Principles SC-01: System and Communications Protection Policy and Procedures SC-04: Cryptographic Key Establishment and Management SC-05: Cryptographic Protection SI-01: System and Information Integrity Policy and Procedures System and Communications Protection Policies, Procedures and Principles
25.	Theft of Data	CA-02: Security Assessments CA-06: Continuous Monitoring CM-03: Security Impact Analysis CM-06: Software Usage Restrictions CP-06: Information System Recovery and Reconstitution IA-01: Identification and Authentication Policy and Procedures IR-01: Incident Response Policy and Procedures IV-02: Audit Logging / Intrusion Detection IV-06: Vulnerability Management MP-01: Media Protection Policy and Procedures MP-03: Media Sanitization MS-12: Encryption PE-03: Physical Access Control PE-04: Monitoring Physical Access SA-04: External Information System Services SC-04: Cryptographic Key Establishment and Management SC-05: Cryptographic Protection SM-05: Supply Chain Agreements SM-07: Third Party Assessment SM-08: Third Party Audits
26.	Theft of Computer	MP-05 Media Transport Physical and Environmental Protection Family
27.	Vulnerabilities in Backup System	CA-06: Continuous Monitoring CP-05: Information System Backup IA-06: Cryptographic Module Authentication Infrastructure & Virtualization Policies, Procedures and Principles IV-06: Vulnerability Management MS-12: Encryption MS-16: Backup Policy RA-01: Risk Assessment Policy and Procedures RA-03: Risk Assessment RA-04: Vulnerability Scanning SC-05: Cryptographic Protection Supply Chain Management, Transparency and Accountability Policies, Procedures and Principles System and Communications Protection Family
28.	Loss of encryption keys	IA-06: Cryptographic Module Authentication MS-12: Encryption SC-05: Cryptographic Protection System and Communications Protection Family
29.	Wireless network breach	AC-04: Information Flow Enforcement AC-10: Permitted Actions without Identification or Authentication AC-12: Wireless Access

Sr. No	Risk and Threat's Description	Control Number and Description
		Identification and Authentication Family
30.	Unauthorized access	AC-09: Session Lock AC-11: Remote Access AC-12: Wireless Access AC-13: Access Control for Mobile Devices AU-08: Protection of Audit Information DS-03: Ecommerce Transactions IA-05: Authenticator Feedback MP-01: Media Protection Policy and Procedures MP-02: Media Access RA-01: Risk Assessment Policy and Procedures SI-03: Malicious Code Protection System and Communications Protection Family
31.	Third party personal breaches	Data Security & Information Life-Cycle Management PS-07: Third-Party Personnel Security SM-07: Third Party Assessment
32.	Improper highlight Security breaches	BC-03: Business Continuity Testing Contingency planning Policies, Procedures and Principles Incident Response Policies, Procedures and Principles IR-01: Incident Response Policy and Procedures IR-04: Incident Monitoring IR-05: Incident Response Assistance IR-06: Incident Response Plan IV-06: Vulnerability Management RA-01: Risk Assessment Policy and Procedures RA-01: Risk Assessment Policy and Procedures SA-04: External Information System Services SM-02: Incident Reporting SM-05: Supply Chain Agreements SM-07: Third Party Assessment SM-08: Third Party Audits
33.	Poor implementation of security plan	BC-02: Business Continuity Planning BC-03: Business Continuity Testing BC-04: Datacenter Utilities / Environmental Conditions BC-06: Impact Analysis BC-07: Retention Policy Business Continuity Management & Operational Resilience Policies, Procedures and Principles Configuration Management Policies, Procedures and Principles Contingency Planning Family Contingency planning Policies, Procedures and Principles Incident Response Policies, Procedures and Principles IR-06: Incident Response Plan IV-05: Information System Documentation Maintenance Policies, Procedures and Principles Planning Family Planning Policies, Procedures and Principles
34.	Interfacing with third parties has vulnerabilities	CA-03: Information System Connections MS-02: Anti-Malware MS-15: Passwords PS-07: Third-Party Personnel Security RA-01: Risk Assessment Policy and Procedures SM-02: Incident Reporting SM-03: Network / Infrastructure Services SM-07: Third Party Assessment SM-08: Third Party Audits
35.	Private information becomes public without customer notice	Configuration Management Policies, Procedures and Principles DS-03: Ecommerce Transactions Incident Response Policies, Procedures and Principles Maintenance Policies, Procedures and Principles Personnel Security Policies, Procedures and Principles RA-03: Risk Assessment RA-04: Vulnerability Scanning SC-04: Cryptographic Key Establishment and Management

Sr. No	Risk and Threat's Description	Control Number and Description
		SI-05: Security Alerts, Advisories, and Directives System and Communications Protection Policies, Procedures and Principles
36.	The Cloud provider terminates or suspend the service	Business Continuity Management & Operational Resilience Policies, Procedures and Principles SA-04: External Information System Services SM-05: Supply Chain Agreements SM-07: Third Party Assessment SM-08: Third Party Audits Supply Chain Management, Transparency and Accountability Policies, Procedures and Principles System and Services Acquisition Policies, Procedures and Principles
37.	Business Continuity	BC-01: Business Continuity Management & Operational Reliance BC-02: Business Continuity Planning BC-03: Business Continuity Testing BC-04: Datacenter Utilities / Environmental Conditions BC-05: Equipment Location and Maintenance BC-06: Impact Analysis BC-07: Retention Policy
38.	Isolation failure	IV-01: Infrastructure & Virtualization Security Policy and Procedure IV-10: Segmentation IV-12: Hypervisor Hardening
39.	Over-usage of shared resources	SA-02: Allocation of Resources
40.	Noncompliance with client instructions relating to data processing	Business Continuity Management & Operational Resilience Policies, Procedures and Principles SA-04: External Information System Services SM-05: Supply Chain Agreements SM-07: Third Party Assessment SM-8: Third Party Audits Supply Chain Management, Transparency and Accountability Policies, Procedures and Principles System and Services Acquisition Policies, Procedures and Principles
41.	Data access and associated logs	Access Control Policies, Procedures and Principles AU-04: Audit Storage Capacity AU-06: Audit Review, Analysis, and Reporting AU-10: Audit Generation Audit and Accountability Policies, Procedures and Principles IV-02: Audit Logging / Intrusion Detection PE-03: Physical Access Control PE-04: Monitoring Physical Access
42.	Ambiguous security responsibilities	AT-01: Security Awareness and Training Policy and Procedures AT-02: Awareness and Training AT-03: Role Based Security Training IR-01: Incident Response Policy and Procedures IR-02: Incident Response Training
43.	Malicious code imbedded in software	SI-03: Malicious Code Protection
44.	Insecure equipment disposal	MP-01: Media Protection Policy and Procedures MP-02: Media Access MP-04: Media Use MP-03: Media Sanitization
45.	Insecure data storage	IA-06: Cryptographic Module Authentication MP-01: Media Protection Policy and Procedures MP-02: Media Access MP-04: Media Use MS-12: Encryption PE-02: Physical Access Authorizations PE-03: Physical Access Control PE-04: Monitoring Physical Access PE-07: Fire Protection PE-08: Temperature and Humidity Controls PE-09: Water Damage Protection

Sr. No	Risk and Threat's Description	Control Number and Description
		PL-01: Security Planning Policy and Procedures PS-06: Access Agreements RA-03: Risk Assessment RA-04: Vulnerability Scanning SC-05: Cryptographic Protection SI-03: Malicious Code Protection
46.	Insufficient cryptographic management	IA-06: Cryptographic Module Authentication SC-04: Cryptographic Key Establishment and Management SC-05: Cryptographic Protection MS-12: Encryption
47.	Economical denial of service	IV-05: Information System Documentation Physical and Environmental Protection Family SA-02: Allocation of Resources SA-04: External Information System Services SC-02: Denial of Service Protection System and Communications Protection Family
48.	Supply Chain Management Failure	SM-01: Data Quality and Integrity SM-02: Incident Reporting SM-03: Network / Infrastructure Services SM-04: Provider Internal Assessments SM-05: Supply Chain Agreements SM-06: Supply Chain Governance Reviews SM-07: Third Party Assessment SM-08: Third Party Audits Supply Chain Management, Transparency and Accountability Policies, Procedures and Principles
49.	Non-compliance with legal requirements	BC-07: Retention Policy Business Continuity Management & Operational Resilience Policies, Procedures and Principles Infrastructure & Virtualization Policies, Procedures and Principles
50.	Noncompliance with data protection law requirements	RA-02: Security Categorization IV-05: Information System Documentation System and Information Integrity Policies, Procedures and Principles
51.	Loss of customer privacy	AC-11: Remote Access AC-12: Wireless Access AC-13: Access Control for Mobile Devices AU-08: Protection of Audit Information CA-06: Continuous Monitoring IA-05: Authenticator Feedback IA-06: Cryptographic Module Authentication IV-06: Vulnerability Management MP-01: Media Protection Policy and Procedures MP-02: Media Access MP-03: Media Sanitization MS-02: Anti-Malware MS-12: Encryption MS-15: Passwords PE-04: Monitoring Physical Access RA-01: Risk Assessment Policy and Procedures RA-03: Risk Assessment RA-04: Vulnerability Scanning SC-05: Cryptographic Protection SI-03: Malicious Code Protection SI-03: Malicious Code Protection SM-7: Third Party Assessment SM-8: Third Party Audits

After detailed mapping of the information security controls on the identified information security cloud related risks, the given above Table 9 definitely shows

that the proposed framework provides assurance to the Higher Education Institutions that it has capability to mitigate cloud related risks adequately.

6.6 IMPLEMENTATION OF SECURED HYBRID CLOUD FRAMEWORK THROUGH AGENT BASED INFORMATION SECURITY FRAMEWORK FOR HYBID CLOUD COMPUTING

In general, an information security approach estimates the risk, where the risk is to occur due to an unusual event, and the associated consequences for cloud Higher Education Institutions. Information Security and Risk Management (ISRA) practices vary among the cloud Institutions and disciplines. There are several approaches to compare existing risk management methods for Higher Education Institutions but their scope is limited while considering stereo type criteria, rather than developing an agent based task that considers all aspects of the associated risk. It is the lack of considering all existing renowned risk management frameworks, their proper comparison, and agent techniques that motivate this research.

In this dissertation, Agent Based Information Security Framework for Hybrid Cloud Computing is developed as an all-inclusive method including cloud related methods to review and compare existing different renowned methods for cloud computing risk issues and by adding new tasks from surveyed methods. The concepts of software agent and intelligent agent have been introduced that fetch/collect accurate information used in framework and to develop a decision system that facilitates the Higher Education Institutions to take decision against threat agent on the basis of information provided by the security agents. The scope of this research primarily considers risk assessment methods that focus on assets, potential threats, vulnerabilities and their associated measures to calculate consequences. The developed framework was implemented using fuzzy inference system based upon fuzzy set theory, and MATLAB® fuzzy logic rules were used to test the framework. The fuzzy results confirm that proposed framework could be used for information security in Higher Education cloud environment. The details about function of Agents in Cloud Computing and Software Agents are given under the sub heading of 6.5 and 6.6 of the Chapter 6 of the Supplementary Material.

6.7 AGENTS BASED INFORMATION SECURITY FRAMEWORK

The most critical roadblock in the development of Cloud Computing is its security and privacy constraints. Although every vender claims that it is providing adequate

security to its customers and various research efforts have been made to cater the needs of security in Cloud computing, but still it is a great challenge for the Higher Education Institutions that deployed Cloud Computing. Security risks and threats always directly decrease the operational processes of the Institutions. During literature review, it is extracted that various Information Security frameworks exist but none of the Information Security framework use Software Agents and Intelligent Agents technology to meet the challenges of Information Security.

This dissertation introduced Software Agents to formulate Information Security framework and used Information Security Metrics that is a valuable tool to measure the performance of the Information Security System. Furthermore, risk management techniques are also used to define the severity level of the risk. In order to deploy the Secured Hybrid Cloud Framework in the Higher Education Institutions, a four stages approach is proposed, as shown in Figure 13**.**

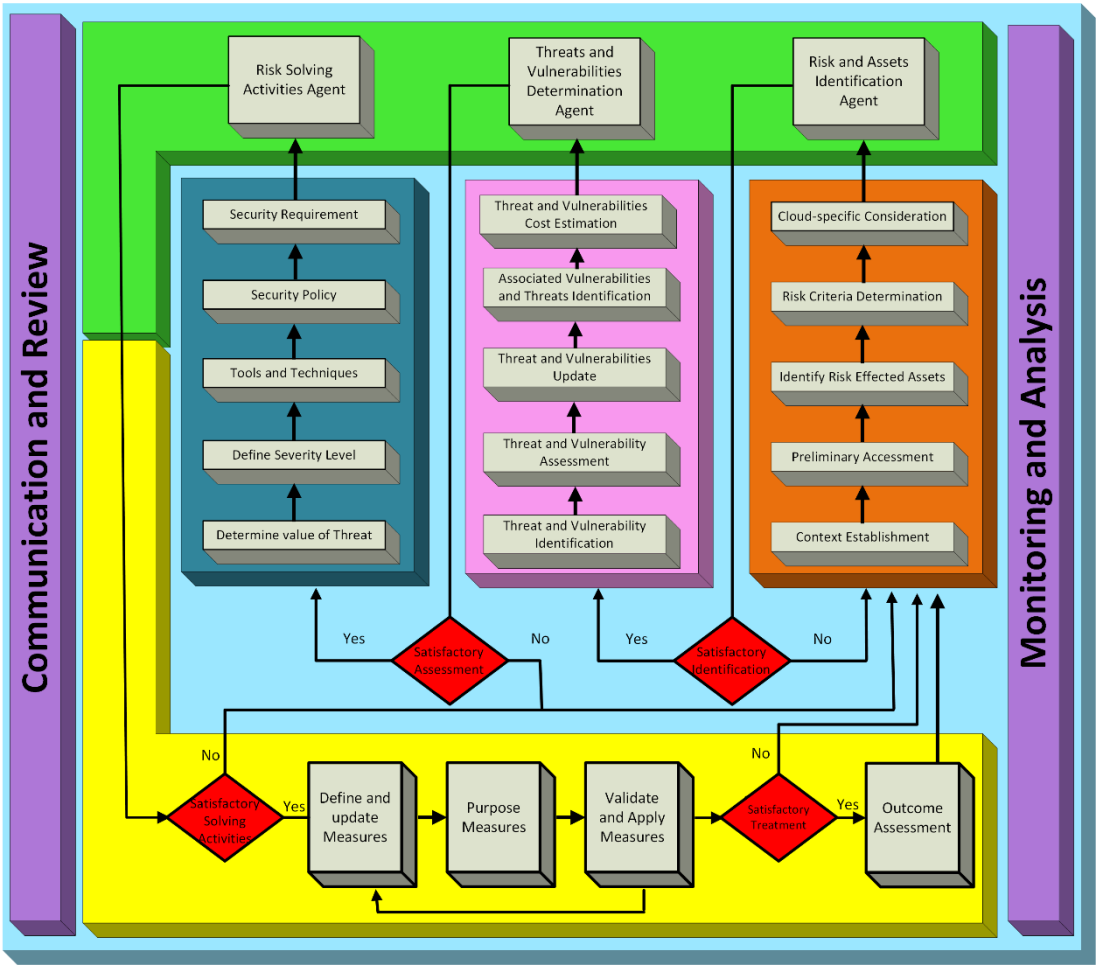


Figure 13. Agent Based Information Security Framework

6.7.1 **Risk and Assets Identification Agent**

The agent initially performs the preliminary assessment by targeting business processes, goals and objectives. Identifies and analyze stakeholders, identifies risk effected assets, estimates its damage cost, identifies owner of the assets, container of the assets, evaluates each and every asset that can be targeted by the risks, threats and vulnerabilities. It identifies potential risks through negotiation and collaboration with other agents over the network, internet, social contacts, security agencies, research portals, research laboratories, forums and groups etc. Segregate risks, define key factors, motivation of the risk, scope of the risk, targets of the risks, and identifies key risk indicators, risk aggregation and its prioritization. Assess and evaluates associate risks with cloud service provider. The details of each task of agent is given as under:

6.7.1.1 Context Establishment

Risks in context to Information Security are always uncertain and its mitigation process cannot be fully achieved until the objectives and strategies of the business are clear. Context establishment means to define the scope of all processes involved in the risk management and also sets the criteria to assess the tasks for the mitigation of risks [135]. The scope of risk management must be within limit of the organizational goals and objectives.

6.7.1.2 Preliminary Assessment

After defining context establishment, the next step is Preliminary Assessment. The target of preliminary assessment is to identify business processes and objectives, identify and enlist the stakeholders that are effected with risk, initially analyse the stakeholders to secure their interests, identify the risk factors, protective factors and document the gathered details about risk [136].

6.7.1.2.1 Business Process and Objective Identification

Business process identification is the part of preliminary assessment wherein all operational activities of the business are defined, applicable rules and policies are also documented [137].

During risk mitigation process, it is necessary to consider and secure the objectives of the owner of organization.

6.7.1.2.2 Identification of Stakeholder

Identification of stakeholder is the process to identify the concerned stakeholders that are required to be contacted at the time of risk mitigation and also make sure their involvement in risk mitigation process to effectively identify and mitigate risks [138] [139].

6.7.1.2.3 Analysis of Stakeholders

The analysis of the stakeholders is the essential part of the preliminary assessment wherein the stakeholders are thoroughly analyzed as per defined criteria of the risk management like their influence and interest in the risk mitigation process [137].

6.7.1.2.4 Personal Data Identification and Mapping

Personal data of the employees, employer and stakeholders is very important to be rescued, secured and recovered. During, preliminary assessment, it would be the part of the risk management to identify the personal data of the stakeholders, mapped the same and thereafter assessed whether it is according to law, policies and rules applicable therein or not? [140].

6.7.1.3 Identify Risk Effected Assets

Identification of assets is very critical process of the risk assessment and it always played a vital role in the risk mitigation [141]. During risk assessment and its mitigation, it is necessary to identify exact assets of the organization that are effected with risk and such record of the assets will further facilitate other tasks of the risk assessment [142].

6.7.1.3.1 Asset Evaluation

The Assets are required to be evaluated according to set criteria like their cost, worth, importance in the information system, who used the assets, timeline of utilization, and effectiveness of the asset in the information system and also its priority [143].

6.7.1.3.2 Identification of Asset's owner

The identification of asset's owner will facilities risk management process to frame its scope and focus target of the risk assessment [143].

6.7.1.3.3 Asset Container Identification

The asset container is the place where assets of the information system resides / stored / transported, and processed [143].

6.7.1.4 Risk Criteria Determination

The decision makers of Information Security Risk Assessment team takes decision on the basis of risk criteria. The risk criteria determines the significance of the risk and categorized the risks in the light of its severity, area of attack, types of assets, stakeholders, mitigation cost and other parameters [144].

6.7.1.4.1 Risk Elicitation

To define risk criteria, it is necessary to identify the risk. There are several ways to elicit the risk. There are several sources of Information security that enlist the current and past risks that can effect on information security [145]. Furthermore, the Information Security Risk Assessment team also elicit real time risks from the Information System.

6.7.1.4.2 Key Risk Indicators

After elicitation of risk, the next step is to identify and define key risk indicators. The key risk indicators are always build on the basis of predefined appetite and information security metrics [144]. If organization compromised these key risk indicators and risk appetite executed.

6.7.1.4.3 Determination of Risk Level

The third stage of risk criteria determination is to determine the level of the risk. For this, ISRA team builds risk scenarios, executes and compiles them, document the consequences and determine the value level of risk [146].

6.7.1.4.4 Risk Aggregation

Risk aggregation is a task that is performed to build link between rolled up risks and integration of high level and low level of risks [146]. ISRA team shall scan each risk according to its risk level and aggregate each individual risk. The purpose of this activity is to reinvestigate each risk and aggregate it according to its potential development.

6.7.1.4.5 Risk Prioritization

It is the task in which significance of each risk is evaluated, each risk mitigation process is prioritized in the light of its severity and cost [145].

6.7.1.5 Cloud-specific Consideration

Cloud related considerations are included in the Information Security Risk Assessment process to study the risks that are related to cloud computing. The proposed framework specialization is that it would be suitable for the cloud

organizations in addition to traditional IT organizations. This task will make sure that during ISRA process, the ISRA team has considered the risks specific to cloud computing [68] [144].

6.7.1.6 Assessment of Cloud Service Provider

The purpose of assessing cloud service provider is to include methods and techniques in Information Security Risk Assessment related to Cloud Service Provider. This task will include Cloud Service Provider's existing security controls and compliance [144].

6.7.1.7 Software Agent Consideration

The Information Security Risk Assessment team shall consider software agent techniques during risk identification, assets elicitation, risk aggregation and prioritization. This task will expedite risk mitigation process by collaborating with other agents over the internet.

6.7.2 **Threats and Vulnerabilities Determination Agent**

The said agent shall identify potential and existing threats and vulnerabilities, document them, thoroughly assess each of them, update about threats and vulnerabilities by coordinating with other agents over the network, find out associated threats and vulnerabilities and also estimate threat damage and mitigation cost [147].

6.7.2.1 Threat and Vulnerability Identification

Vulnerability and Threat identification is the process of identifying relevant threats and vulnerabilities of an asset and for organizations that exploit information security. The said task identify each threat and vulnerability, quantify and rank each of them in the system. This task also covers relevant methods and approaches to find credibility and severity of potential vulnerability and threat [147].

6.7.2.2 Threat and Vulnerability Assessment

Vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system [146] [147]. The Information Security Risk Assessment methods further guided to expand the assessment techniques and tools to estimate each threat and vulnerability willingness and motivation to attack. During threat and vulnerability assessment, the capability of each threat is gaged to compare with risk mitigation capability of the information security system and

furthermore, the capacity and potential of each threat is assessed in terms of the resources used by the risk to attack [148]. The assessment task documents the duration and consequences of each attack.

6.7.2.3 Threat and Vulnerability Update

The identified and assessed threats and vulnerabilities are required to be updated in the system so that the old information about these threats and vulnerabilities must not be used again [147] [148]. The software agents of the framework will communicate updates to other agents over the internet and receive updates from other agents to keep information to update.

6.7.2.4 Associated Vulnerability and Threat Identification

Various threats are interconnected with other threats and attack the system in collaboration with other threats. Therefore, it is necessary to identify and update all links and associated vulnerabilities and threats [148]. The associated threats and vulnerabilities are required to be assessed with the mechanism used for main threats and vulnerabilities.

6.7.2.5 Threat and Vulnerability Cost Estimation

Every threat mitigation is required to be assessed in such a manner that system should calculate its damage cost and the cost required to mitigate it. Various threats have high mitigation cost and very low severity level as compared to cost of the damage they do. The system, thereafter, accordingly set their mitigation priority as very low and often don't mitigate them due to their high cost [144] [145].

6.7.3 **Risk Solving Activities Agent**

The risk solving activities are performed after thorough investigation of risks, threats and vulnerabilities, associated assets, stakeholders, owners and business processes. The agent shall, before moving on to the next step, must first determine the value of the threat, define severity level of the risks and threats, find appropriate tools and techniques to address potential risks and threats, find applicable policies defined in the method, existing security requirements and then find alternate solutions to resolve the issues.

6.7.3.1 Determine Value of Threat

Threat value determination is actually the assessment of the damage done to the assets, personal information, organizational information and physical infrastructure

[149]. Such value can be assessed through building scenario of potential threat and then assessing the damage it causes.

6.7.3.2 Define Severity Level

It is a continuous process which contains the defined/set severity of each threat agent based on the collected information, security requirements, established policies and tools required to mitigate the threat agent [150]. The severity level will facilitate the organization to set the priorities of action to be taken if more than two threat agents attack at the same time.

6.7.3.3 Tools and Techniques

In order to enforce the security policies against each threat agent, the analysis of tools and techniques lead towards the appropriate solution of threat agent. Different websites, news groups, dashboards, forums and research papers may be used to dig out the most suitable tools.

Although the performance of all tools and techniques that are used for cloud are not equal, but in this section, the framework will find the most widely accepted and used tools for Cloud computing risks mitigation. For example HyTrust's virtual management and CohesiveFT sells cloud security tools [144].

6.7.3.4 Security Policy

After determining the security requirements, establishment of Security policy is necessary. Each security policy is established against each threat agent and its respective security requirements are taken care of. Security policies must be cleared and rectified for the threat agent [143] [146]

6.7.3.5 Security Requirement

In order to mitigate the threat agents, the security goals and security requirements of the threat agent should be determined [151]. The number of actions to be taken to reduce the severity of the particular threat agents have to be defined. Cloud Security Alliance (CSA) has introduced the Cloud Security Metrics V3.01 which is very useful for the Cloud organizations to define the security requirements against identified risks.

6.7.3.6 Agents to find out alternate solution

The agent shall find out alternate solutions available over the network, suggested by other organizations, gathers through collaboration and negotiation with other agents,

research groups and forums, industry, research laboratories, discussion with information security expert, during communication and review task etc.

6.7.4 **Measures**

Measures is the final stage of this framework wherein framework update existing measures in system, identify controls to apply on risk, before applying appropriate controls, assess their previous effectiveness and finally purpose measure to mitigate risks, threat and vulnerabilities. The final outcome of the measures shall again be verified.

6.7.4.1 Define and update Measures

After intensive work out on risks and assets, threats, vulnerabilities, stakeholders, owners, business goals, process and objectives, find out relevant risk mitigation techniques, tools, policies, requirements and alternate solutions, it is necessary to define and update existing measures if necessary [152].

6.7.4.1.1 Control Identification

Before applying measures, identification of appropriate controls is very critical process. The system already has a number of relevant controls against the risks, but in case of newly identified risks, it is necessary to identify relevant controls from the existing control's database or otherwise agents will contact other agents to get controls for risks [144] [153].

6.7.4.1.2 Control Efficiency Assessment

This task is a tricky and very critical one as it assess the effectiveness of the already proposed controls for the mitigation of risk. If the control already applied on the same type of risk, then its previous effectiveness would be considered before its selection, otherwise agent would be activated to identify alternative controls for concerned risk [145].

6.7.4.3 Purpose Measures

After identification and assessing efficiency of the existing appropriate controls for the risk mitigation, measures shall be purposed. The Information Security Risk Assessment team shall use one measure against one risk or may use more than one measure and vice versa. Therefore, the ISRA team is required to keenly focus on this task.

6.7.4.4 Validate and Apply Measures

To validate the measures, it is required to identify the outcome of the measures, so first ISRA team must identify the likely outcome of the risks, threats, vulnerabilities and assets if security breaches and team also required to estimate the cost of damage if potential event occurs [154].

After assessing outcome of potential event and before applying measures, it is mandatory to validate the measures through reliable methods, and techniques. In case of measures not validated, the measures criteria is required to be evaluated again [147].

6.7.4.5 Outcome Assessment

This is the final stage of the Information Security framework. The outcome of the measures shall be assessed to check the effectiveness of the controls and applied measures [144] [155]. If the risk, threat and vulnerability is completely removed, then event shall be documented along-with concerned risks, assets, vulnerabilities, threat, applied measures, techniques, tools, methods, rules, policies, cost, severity level etc., otherwise the whole process will be repeated to accurately identify, validate and apply measures.

6.7.5 **Communication and Review**

The communication and review is the continuous task throughout information security risk assessment method. The risk, vulnerability, threat, concerned assets, outcome of the method and its outcome assessment shall be shared with other agents. The sharing of the said information and details with other agents of the organizations will update their system methods to mitigate such types of risks in future [156]. The other organizations will review the outcomes of Information Security Risk Assessment and update their system if necessary. Each cloud organizations should communicate risk and threat assessment results with other stakeholders either formally or informally.

6.7.6 **Monitoring and Analysis**

Monitoring and Analysis is also a continuous process that keeps working from the pre-assessment to outcome assessment tasks. In this task, all threat and risk activities are observed and examined minutely, and if the team feels necessary, make changes and update the method to make it more comprehensive [157]. The Information

Security Risk Assessment method should be reviewed, updated as and when new threat and risk identified or this method applied to mitigate the risk and threat. The ISRA team should keep update security requirements, tools & techniques, policies and applicable measures.

6.8 INFORMATION SECURITY RISK ASSESSMENT METHODS

During intensive literature review regarding Information Security Risk Assessment, researcher reviewed seven renowned Information Security Risk Assessment (ISRA) methods that have lot of common points and were developed specifically for risk assessment. These methods are well documented and currently, various organizations are following these methods to mitigate risks. The brief about these seven methods are given under the sub heading of 6.7 of the Chapter 6 of the supplementary Material.

6.9 EVALUATION OF EXISTING ISRA METHODS WITH ABISF

During literature review, studied different stereo-type criteria to compare existing Information Security Risk Assessment methods which uses only basic risk assessment techniques as benchmark and overlook the tasks that their proposed framework do not covers. The authors studied seven renowned Information Security Risk Assessment frameworks thoroughly and written down their common and distinguished risk assessment points to formulate a comprehensive criteria for the evaluations of existing ISRA methods. The authors critically analyzed each of the task covered under study method, collected the relevant tasks from other ISRA methods and thereafter, combined them to formulate one task that covers all approaches opted by other methods. The said approach is very comprehensive as the developed criteria is taken from surveyed ISRA methods. Developed a simple criteria to quantify each ISRA method and the same criteria has been implemented on proposed ABISF to validate it.

A developed criteria is given in Table 10. Each method and its associated task will be selected and passed through criteria to get the results.

Table 10. ISRA Method Evaluation Criteria

Value	Description	Remarks
0	Not addressed	The method does not support task
1	Partially addressed	The method partially support task

Value	Description	Remarks
2	Completely Addressed	The method completely support task

The developed criteria implemented on seven renowned ISRA methods and their scores compared with ABISF to validate its reliability and effectiveness. The given Table 11 is showing the comparison.

Table 11. Comparison of Agent Based Information Security Framework (ABISF) with (ISRA) frameworks

Assessment Stage	Tasks	ABISF	NSMROS	CIRA	FAIR	ISO/IEC 27005:2011	NIST 800-30	OCTAVE A	RISK IT	Row Total
Risk and Assets Identification Agent	Context Establishment	2	2	2	1	1	2	2	2	**14**
	Preliminary Assessment	2	2	2	1	0	2	2	2	**13**
	Business Process and Objective Identification	1	0	0	2	2	0	2	2	**9**
	Identification of Stakeholder	1	0	2	2	2	0	1	2	**10**
	Analysis of Stakeholders	1	0	2	2	2	0	1	0	**8**
	Personal Data Identification and Mapping	2	0	1	1	1	1	1	0	**7**
	Identify Risk Effected Assets	2	2	2	1	2	2	1	1	**13**
	Asset Evaluation	2	2	2	2	2	2	2	2	**16**
	Identification of Asset's owner	2	0	2	1	2	0	2	0	**9**
	Asset Container Identification	2	0	0	2	0	0	2	0	**6**
	Risk Criteria Determination	2	1	2	1	2	1	2	2	**13**
	Risk Elicitation	2	2	1	2	2	2	2	1	**14**
	Key Risk Indicators	2	0	0	2	1	1	1	2	**9**
	Determination of Risk Level	2	0	0	2	2	2	1	2	**11**
	Risk Aggregation	2	1	0	0	2	2	1	2	**10**
	Risk Prioritization	2	2	2	0	2	2	2	2	**14**
	Cloud-specific Consideration	2	0	0	2	0	1	0	0	**5**
	Assessment of Cloud Service Provider	2	0	0	1	0	1	0	0	**4**
	Software Agent Consideration	2	0	0	0	0	0	0	0	**2**
	Sub-Total	**35**	**14**	**20**	**25**	**25**	**21**	**25**	**22**	
Threats and Vulnerabilities Determination Agent	Threat and Vulnerability Identification	2	1	1	1	2	1	1	1	**10**
	Threat and Vulnerability Assessment	2	0	0	1	2	1	0	0	**6**

	Threat and Vulnerability Motivation Strength	1	0	2	0	2	2	2	1	**10**
	Threat and Vulnerability Capability	1	0	1	2	1	0	0	0	**5**
	Threat and Vulnerability Capacity	1	0	1	1	1	0	1	0	**5**
	Threat Attack Duration	2	0	0	2	1	0	0	2	**7**
	Threat and Vulnerability Update	2	1	0	2	2	2	1	1	**11**
	Associated Vulnerability and Threat Identification	1	0	0	1	1	1	1	2	**7**
	Threat and Vulnerability Cost Estimation	1	1	1	1	2	2	2	2	**12**
	Agents to maintain Threat and Vulnerability	2	0	0	0	0	0	0	0	**2**
	Sub-Total	**15**	**3**	**6**	**11**	**14**	**9**	**8**	**9**	
Risk Solving Activities Agent	Determine Value of Threat	2	1	1	1	2	1	1	1	**10**
	Define Severity Level	2	0	1	2	2	1	1	1	**10**
	Tools and Techniques	2	1	2	1	2	2	1	1	**12**
	Security Policy	2	1	1	2	2	1	1	1	**11**
	Security Requirement	2	0	2	1	1	2	2	1	**11**
	Agents to find out alternate solution	2	0	0	0	0	0	0	0	**2**
	Sub-Total	**12**	**3**	**7**	**7**	**9**	**7**	**6**	**5**	
Measures	Define and update Measures	2	2	1	1	2	2	1	1	**13**
	Control Identification	1	1	1	0	1	2	1	0	**7**
	Control Assessment	2	0	0	0	0	0	0	0	**2**
	Control Efficiency Assessment	2	0	1	0	2	1	0	1	**7**
	Purpose Measures	2	2	2	2	2	2	1	1	**14**
	Validate and Apply Measures	2	2	1	1	2	2	2	1	**13**
	Outcome Assessment	2	2	1	0	2	2	2	1	**12**
	Sub-Total	**13**	**9**	**7**	**4**	**11**	**11**	**7**	**5**	
Grand-Total		**75**	**29**	**40**	**47**	**59**	**48**	**46**	**41**	

After summing the score of four stages vertically, the results show that ABISF has obtained highest score whereas on the other hand, the ISO/IEC 27005:2011 is the second in rating.

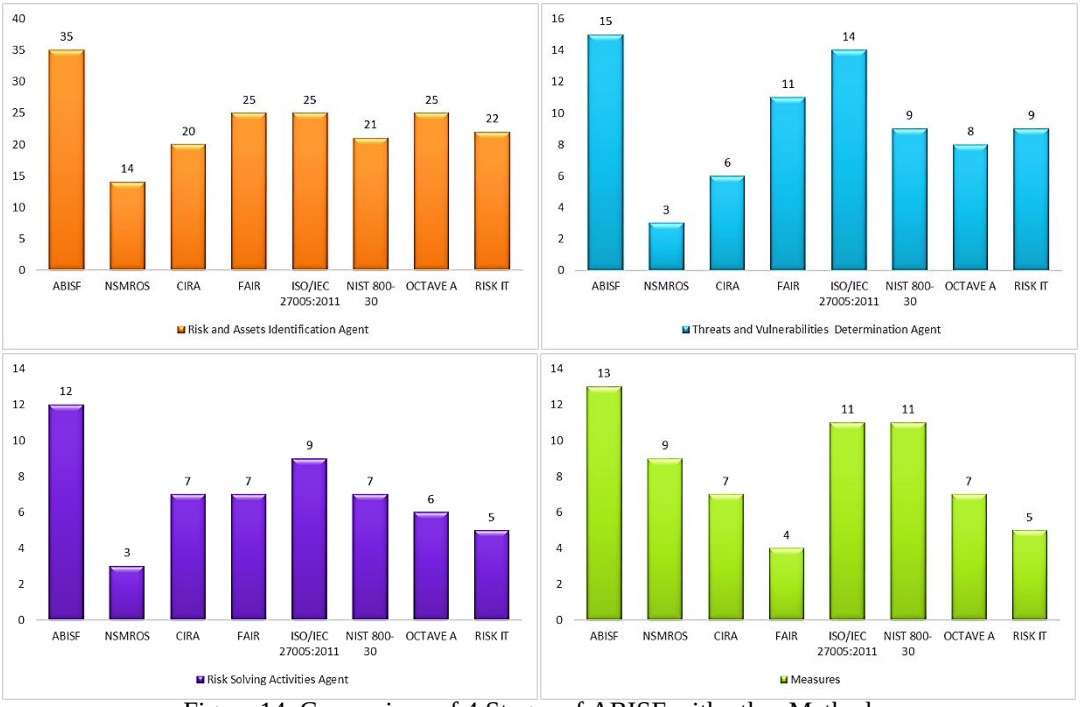


Figure 14. Comparison of 4 Stages of ABISF with other Methods

The NIST SP 800-30, FAIR and OCTAVE A are on third, fourth and fifth position in rating with one point scoring difference. The results of ISO/IEC 27005: 2011 clearly states that it is a comprehensive method and Industry recommends it.

Although OCTAVE A has many citations, a number of researchers used this method in their research but results revealed that this framework still needs improvement. The results of NSMROS are not unexpected, during its study, noticed its effectiveness and loopholes.

It is also noticed that NSMROS is immature ISRA and it was built to cater the needs of specific areas not to cover all Information Security Risk Assessment areas that a comprehensive ISRA should have but even then, it is concluded in comparison to inform the readers about which areas still need improvement.

The Figure 14 presents the detailed comparison of 4 stages of Agent Based Information Security Framework with seven surveyed methods. The said figure clearly depicts that every stage of the ABISF has scored higher points than other methods. In Table 11, it was summarized the scores of each task horizontally, to get a clear picture of which task is mostly addressed in the surveyed methods. In Risk and Assets Identification stage, Asset evaluation is the task that most of the methods included in their risk mitigation process. Thereafter, Context Establishment, Risk Prioritization, and Risk Elicitation scored equal marks in the Risk and Assets

Identification stage. In the Threats and Vulnerabilities Determination stage, Threat and Vulnerability Cost Estimation scored 12 highest points which indicates that it is the task that most of the methods included in their list while addressing threat and vulnerability. Similarly, Tools and Techniques is the most preferred task while performing risk solving activities. Finally, purpose measure is the task that opt every method while mitigating risks from information system. The horizontal scores of the Table 11, helps the Information Security Officers and researchers determine which task is highly recommended by the surveyed methods and which task requires their attention on priority bases.

6.10 EVALUATION OF AGENT BASED INFORMATIN SECURITY FRAMEWORK

Fuzzy logic is a dominant method used to handle inaccurate and inexact data. It describes, develops and implements complex control systems that facilitates the designers to develop such systems with simple and intuitive methods.

The Figure 15 is presenting fuzzy model comprises of four input modules. As stated earlier, fuzzification is the first stage of the model, it accepts crisp values and convert them to fuzzy values. Fuzzy values are obtained on the knowledge of users, processed by the inference engine, and then transformed into crisp values by Defuzzification.

Fuzzy logic has different fuzzy sets and membership functions. Membership functions have values between 0 and 1. At this time, there are eleven membership functions available in MATLAB®. For the evaluation of Agent Based Information Security Framework, considered only 1 membership function i.e. Triangular.

In 2011, Fuzzy inference has been used for risk assessment using risk matrix [27], whereas in the same year, authors focused on fuzzy logic for risk assessment [27]. The authors applied fuzzy logic for risk assessment and decision making [28]. Similarly, fuzzy logic opted and used by various researchers for risk assessment [27] [29] [30] [31].

Before evaluation of proposed framework, it is required to design a system using fuzzy inference system that is based upon fuzzy set theory i.e. if-then rules and logical reasoning. The first stage of the designed system is to determine input and output variables, given in Figure 15. The second stage of fuzzy interface is the data

collection for input variables. All the input variables have further input feeding variables that are mentioned in the Figure 13**.**

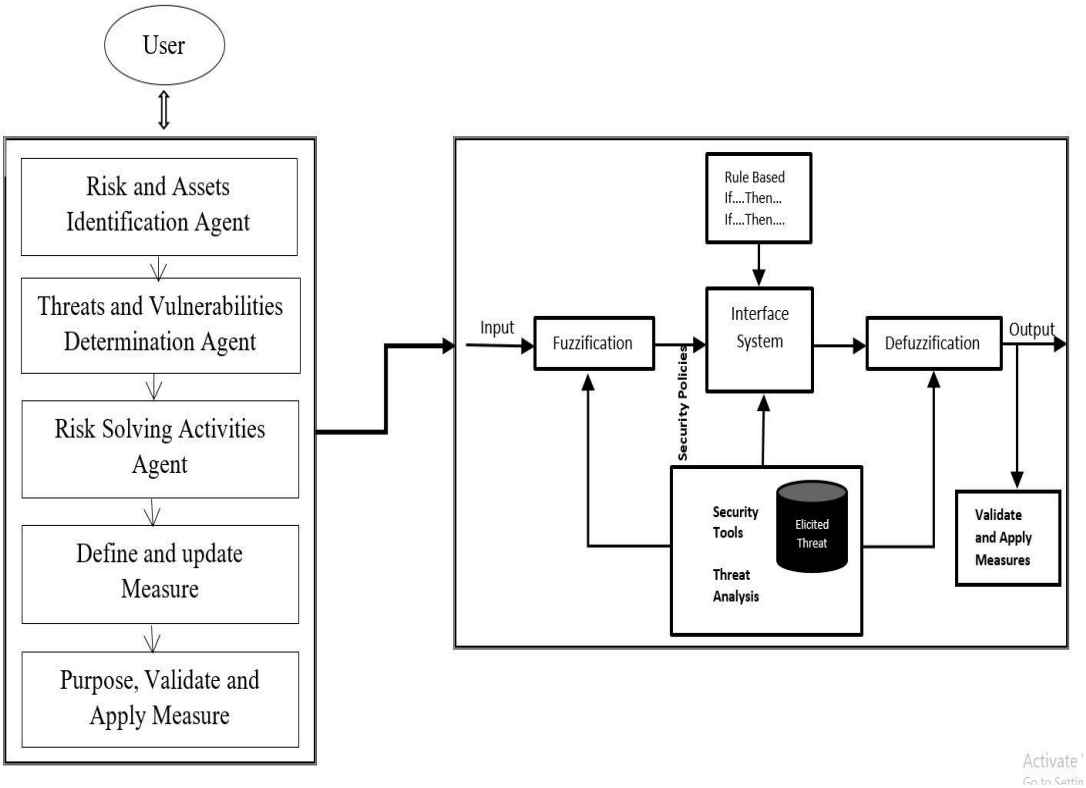


Figure 15. Fuzzy Based Information Security Framework (FBISF)

The third stage of fuzzy is to propose Information Security Framework. FBISF has forward and backward chaining. The model – is given in Figure 15 – has Risk and Assets Identification Agent (RAIA), Threats and Vulnerabilities Determination Agent (TVDA), Risk Solving Activities Agent (RSAA), Define and update Measure (DUM), Purpose, Validate and Apply Measure (PVAM) and Database consists of information about Threats and fuzzy rules, fuzzification, inference engine and defuzzifier.

The inference has been formed by grouping a number of fuzzy rules. 243 fuzzy rules were taken into consideration with the combination of linguistic variable values, and these rules are not mentioned in paper due to its length constraints. The second last step is Defuzzification which acts as mediator between fuzzy control and inference system. Regular Defuzzification methods (Mamdani) were opted. The last step is implementation of fuzzy rules through MATLAB®. In this study, four input variable and one output, are used as shown in Figure 16. The FBISF has been implemented to get decision. Implementation is performed with the support of fuzzy norms. Membership function are assigned to both, input and output values using

MATLAB®. Different Information Security risks and threats have been recorded and processed.

Total 3^5=243 rules are formulated and assessed by MATLAB Rule editor and viewer by using IF- AND- THEN logic. Figure 17 shows MATLAB Rule viewer for cloud computing.

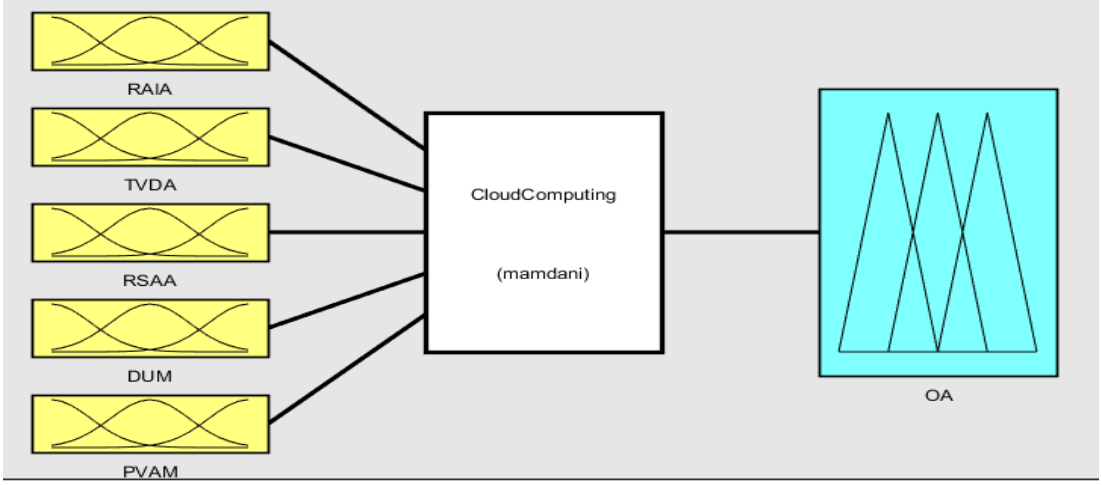


Figure 16. Fuzzy Logic Controller using Fuzzy Based Logic Inference System Editor for Cloud System.

In this Fuzzy Logic cloud computing system, researcher have taken five variables as input variables and Outcome Assessment (OA) as output variable. There are three membership functions against each input. Output outcome assessment has also three membership functions. Figure 17 shows these input and output variables. The ranges of membership functions are taken as 0 to 10 for each input.

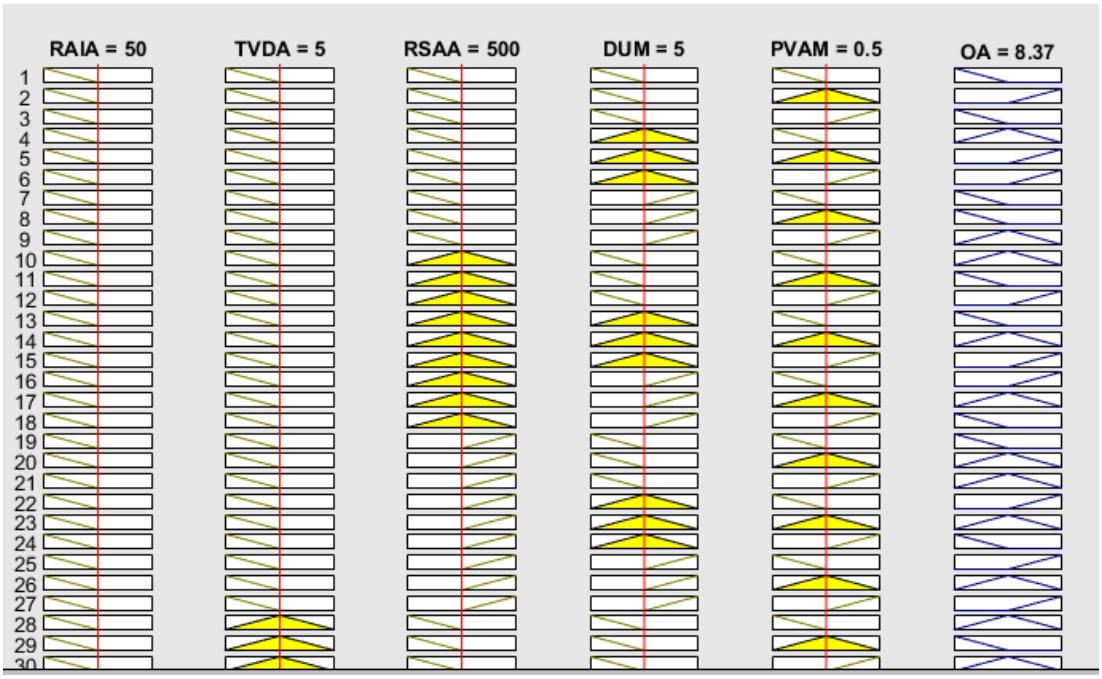


Figure 17. MATLAB Rule view

Here the 3D graphs of surface viewer for the RAIA, TVDA, RSAA, DUM, PVAM and output OA are presented in the Figure 18 (a, b, c, d, e, f, g, h, I and j). Figure 18(a) shows the dependency of output decision on DUM and RSAA. Figure 18(b) shows the dependency of output decision on PVAM and RSAA. Figure 18(c) shows the dependency of output decision on DUM and TVDA. Figure 18(d) shows the dependency of the output decision on the RSAA and the TVDA. Figure 18(e) shows the dependency of output decision on PVAM and RAIA. Figure 18(f) shows the dependency of output decision on DUM and RAIA. Figure 18(g) shows the dependency of output decision on RSAA and RAIA. Figure 18(h) shows the dependency of output decision on TVDA and RAIA. Figure 18(i) shows the dependency of output decision on TVDA and PVAM and Figure 18(j) shows the dependency of output decision on PVAM and DUM. A user who intends to take decision on the identified threat may rely on identified dependencies. Therefore, output decision was taken on the values of RAIA = 50, TVDA = 5, RSAA = 500, DUM 500, PVAM =0.5 and according to Mamdani's model output was obtained 8.37. The Mamdani's model is very useful for these crisp values of Fuzzy Logic cloud computing system. The results of Mamdani's model and the MATLAB simulated value are in Table 12.

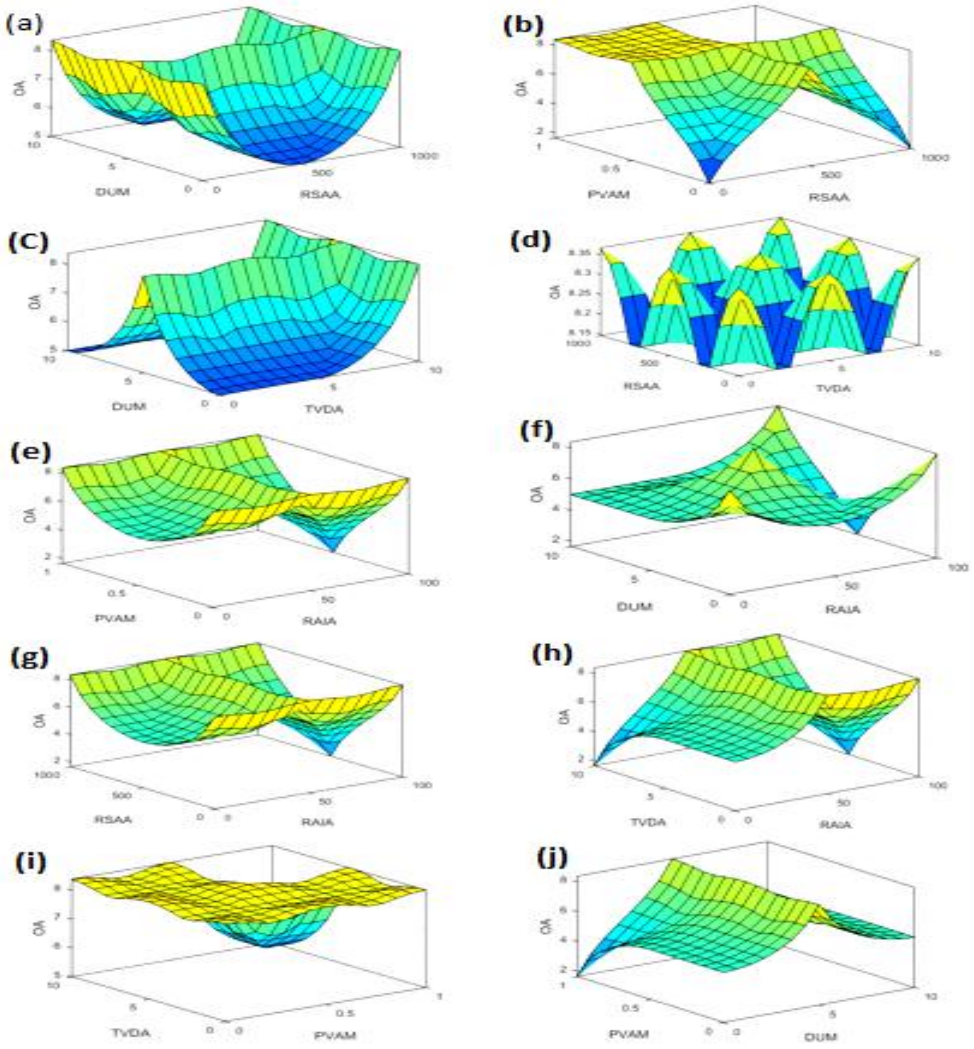


Figure 18. 3D Graphs of Sample Solution

With a greater accuracy and higher output performance, Fuzzy Logic cloud computing system was established. Therefore, systems with dynamic control and complexity can be successfully solved, analyzed and developed. Hence, the rules were obtained through this system for the output decision. Therefore this novel system was confirmed for precise values of the all the inputs.

Table 12. RESULT COMPARISON

Category	Decision
Mamdani's value	7.46
MATLAB simulation	7.48
Difference	0.02
Error percentage	0.26%

The difference measured in the designed and the simulated value is just 0.26%, which is insignificant. It confirms that proposed framework could be used to take decisions on the security threats.

The agent based information security framework facilitates the Higher Education Institutions to use multi-agent techniques in the identification of a threat, develop security metrics through agents and analyse threat agents. The ABISF is implemented in MATLAB® and evaluated by fuzzy set theory and found viable solution.

The development of the Secure Hybrid Cloud Framework provides many benefits for both Higher Education Institutions and the information security public. This section highlights the benefits that this framework adds to its principles, as well as how to improve the information security in Higher Education Institutions.

The Secure Hybrid Cloud Framework offers many advantages beyond the benefits of the previously created information security framework. The significant change observed throughout the world in the adoption of information and information technology by organizations has increased the need to ensure adequate information security and implementation. However, the information security described above simply addresses typical information security issues. Therefore, it can be said that this is no longer sufficient to guide organizations in this regard. Thus, information security is very useful because it specifically addresses the information security that still retains many of the vital concepts described in the predetermined frameworks. In addition, these Information Security frameworks specifically addresses critical success factors and does not guide the implementation of information security frameworks. Therefore, the developed frameworks in this research / study provide Higher Education Institutions a strong foundation for their development, implementation and management of Information Security, which complies with best practices and International principles.

Upshot, the primary goals of this dissertation was to develop secure hybrid cloud framework that could meet the information security principles and facilitate the Higher Education Institutions to secure their infrastructure within limited resources and expenditure. With the development of Secured Hybrid Cloud Framework for Higher Education Institutions in Pakistan and Agent Based Information Security Framework, this has been achieved.

This chapter described a number of Information Security Framework principles which are evident from the literature of this dissertation. The existing Information Security Standards are evaluated by using risks management techniques and criteria

to know the effectiveness of their controls for Cloud Computing. To cater the needs of Information Security for Higher Education Institutions of Pakistan, the framework was introduced with 24 domains. Each domain of the framework is described in detail along-with associated cost effective and essential Information Security Controls and finer working.

Moreover, as some Higher Education Institutions have minute expertise and experience in the implementing of security framework, therefore, an agent based information security framework is developed by using information security risk management techniques to implement the SCHF in Higher Education Institutions.

Subsequently, the benefits of this framework were highlighted. These benefits have accumulated from improvements in the existing information security framework, in addition to the comprehension of principles.

Chapter 7: Evaluation and Prioritization of Security Controls

This Chapter describes about the detailed steps involved in the evaluation and prioritization of Information Security Controls which were developed in the preceding chapter. It also describes the different Multi Criteria Decision Making techniques, comparing these techniques; develop Fuzzy TOPSIS technique to address the problem, criteria for the evaluation of information security controls and alternatives. It also elaborates how the developed alternatives were weighted and scored accordingly. Finally, it provides the calculations to complete Fuzzy TOPSIS.

7.1 SELECTION AND PRIORITIZATION OF INFORMATION SECURITY CONTROLS

Proper assessment of Information Security Controls is essential for Higher Education Institutions to maintain their information resources. The literature highlighted several problems, gaps, deficiencies and / or lacks within traditional Information Security Control Assessment methodologies that prevent the effective evaluation of Information Security Control in Higher Education Institutions. To mention one, the selection of Information Security Controls in Higher Education Institutions by using traditional methods was determined on the basis of yes or no values. The HEIs subjectively base their selection process, regardless of whether the Information Security Control is relevant or irrelevant.

Information Security Controls which are determined to be relevant and implemented. There are other methodologies of assessment of Information Security Control that indicate improvement. For example, HEIs do not adequately take into account the Institution's limitations (for example, costs, availability of resources, suitability, etc.), while other methodologies leave the Information Security Controls identification on the disposal of the users, which results in the possible inclusion of Information Security Controls that are not necessary to possess or exclude of desired ones.

Furthermore, there are a few formal evaluation methodologies that base their Information Security Controls selection on ad hoc or randomized approaches, again leading to the possible inclusion of Information Security Controls and / or the

exclusion of the required Information Security Controls. To continue, Information Security Controls assessment methodologies based on checklists could result in an imperfect information security strategy. For a complete description of the flaws observed in the literature review on Information Security Controls assessment methodologies.

The shortcomings identified above do not only affect the Information Security Controls selection process, but also influence the overall protection of integrity, integrity and availability of information [158]. Owing to lack of proper information security over valuable, critical and sensitive may allow misuse of data, loopholes in security, breach of information and also may provide opportunities to attackers.

Traditional Information Security Control assessment practices, like Risk Analysis and Management (RAM), OCTAVE, NIST, etc. Adhoc approaches and checklists, among others should be strengthened and improved to help organizations with their Information Security Control selection process. Information Security Control assessment methodologies do not promote the evaluation, selection or definition of Information Security Control priorities in HEIs regarding their information.

The actual implementation of the information system security requires identification, assessment and prioritization of the most appropriate Information Security Control [159], taking into account the problems outlined above. To enhance the effectiveness of evaluation and selection process for the Information Security Control in HEIs, a new, effective and an efficient evaluation method is required to be developed.

7.2 BACKGROUND WORK

Several reasons have been presented to explain the lack of effectiveness in the evaluation, selection and implementation of the Information Security Control process. Based on [160] Information Security Control in HEIs which is based on implementation can be an obstacle to make progress. For example, panel participants in the 1993 ICIS conference indicated that the implementation of Information Security Control can slow down the production and thus the render employees' work ineffective [161]. Employees can see the Information Security Control as an interruption of their daily activities [162] and therefore tend to ignore their implementation to be effective and efficient with their daily work activities.

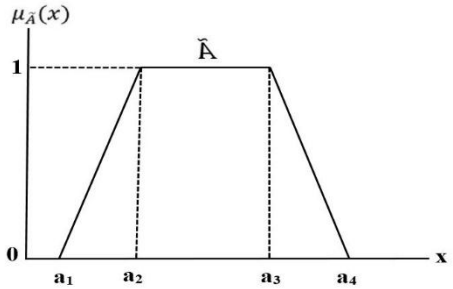
According to [158], organizations must identify and implement appropriate controls to ensure the security of adequate information. In [163], the researcher emphasized the fact that "different organizations have different security needs and different security requirements and objectives". Furthermore, [164] insist that there is no single information security solution that can be adapted to all HEIs. As a result, the Information Security Control must be wisely selected to meet the precise needs of the HEIs. The Information Security Control is an important step to provide an adequate level of security in HEIs [34]. The details about the previous approaches used for the selection of information security controls, Fuzzy TOPSIS method and the Criteria for Information Security Control Evaluation and Selection are given under the sub heading of 7.1, 7.2 and 7.3 respectively of Chapter 7 of the Supplementary Materia.

7.3 THE PROPOSED METHOD

In Decision Making process, decision makers give subjective judgments based upon their relevant experience and knowledge in an ambiguous statement. Like, Good, Very Good, Excellent, important, poor, and so on, given in linguistic terms. To deal with the ambiguous and vague statements of the human, linguistic variables are used to express the membership functions as given in the fuzzy set theory [165]. The inventor of Fuzzy Logic proposed methodology for decision making in fuzzy environment to redress lack of precision, and rating of alternatives issues. In this section, defined the linguistic variables, calculated the weight and TOPSIS procedure are defined.

7.3.1 **Linguistic Variables and Fuzzy Numbers**

The linguistic variable is a variable which values are given in human understandable words, phrases, sentences expressed in an artificial language. The membership function is mapped as $\mu_{\tilde{A}}(X): X \rightarrow [0,1]$. The membership functions of Trapezoidal



fuzzy number $\tilde{A}$ can be expressed as follow:

Figure 19. Trapezoidal Fuzzy Number

$$\mu_{\tilde{A}}(x) = \begin{cases} 0,\ x \leq \\ (x - a_1) \ / \ (a_2 - a_1),\ a_1 \leq x \leq a_2 \\ (a_4 - x) \ / \ (a_4 - a_3),\ a_3 \leq x \leq a_4 \\ 1, a_2 \leq x \leq a_3 \end{cases} \quad (1)$$

In this dissertation, these types of expressions are opted to evaluate, rank and prioritize the Information Security Controls against each criterion, with respect of Trapezoidal Fuzzy Number (TrFN) as used by [166] [167]. A TrFN is a Fuzzy set $\tilde{A}$ on X.

Here in this dissertation, a trapezoidal fuzzy number is denoted as $\tilde{A} = (a_1, a_2, a_3, a_4)$, where $(a_1, a_2, a_3, a_4)\ \epsilon\ R\ where\ a_1 < a_2 < a_3 < a_4$ which denotes the smallest and largest possible value respectively as shown in Figure 19. The

Table 13 and Table 14 show the corresponding TrFNs for each linguistic variables against input and output criteria. The Figure 20 to Figure 26 are about Linguistic variables for the fuzzy rates of alternatives.

Table 13. TrFNs against each Linguistic Variables of input criteria

Criteria	Linguistic Variable	Trapezoidal Fuzzy Number (TrFN)
Effectiveness	Poor	(0.0, 0.0, 0.1, 0.2)
	Satisfactory	(0.1, 0.3, 0.3, 0.5)
	Good	(0.4, 0.6, 0.6, 0.8)
	Excellent	(0.7, 0.9, 1.0, 1.0)
Implementation Time	High Time	(0.0, 0.0, 0.2, 0.4)
	Moderate Time	(0.3, 0.5, 0.5, 0.7)
	Less Time	(0.6, 0.9, 1.0, 1.0)
Mitigation Time	Higher Time	(0.0, 0.0, 0.2, 0.4)
	Moderate Time	(0.3, 0.5, 0.5, 0.8)
	Shorter Time	(0.7, 0.9, 1.0, 1.0)
Maintenance Frequency	Frequent	(0.0, 0.0, 0.2, 0.4)
	Seldom	(0.3, 0.5, 0.5, 0.8)
	Never	(0.6, 0.9, 1.0, 1.0)
Risk	High	(0.0, 0.0, 0.2, 0.4)
	Medium	(0.25, 0.5, 0.5, 0.75)
	Low	(0.6, 0.9, 1.0, 1.0)
Budgetary Constraints	High	(0.0, 0.0, 0.1, 0.3)
	Moderate	(0.2, 0.5, 0.5, 0.8)
	Small	(0.7, 0.9, 1.0, 1.0)

Table 14. TrFNs against each Linguistic Variables of output criteria

Out Criteria	Linguistic Variable	Trapezoidal Fuzzy Number (TrFNs)
ISC Selection	Not Important	(0.0, 0.0, 0.05, 0.2)
	Little Important	(0.1, 0.25, 0.25, 0.4)
	Average Important	(0.3, 0.45, 0.45, 0.6)
	Very Important	(0.5, 0.65, 0.65, 0.8)

	Extremely Important	(0.7, 0.9, 1.0, 1.0)

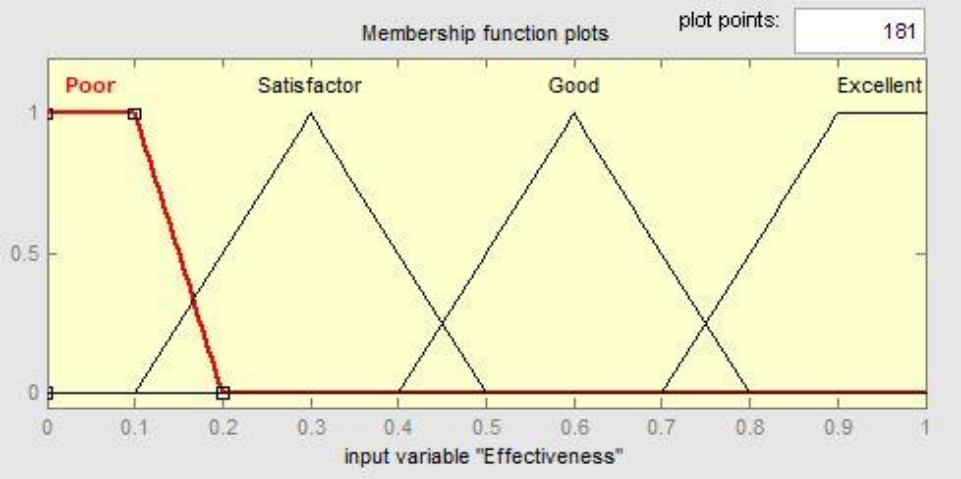


Figure 20. Linguistic Variables of Effectiveness for the Fuzzy Rates of Alternatives

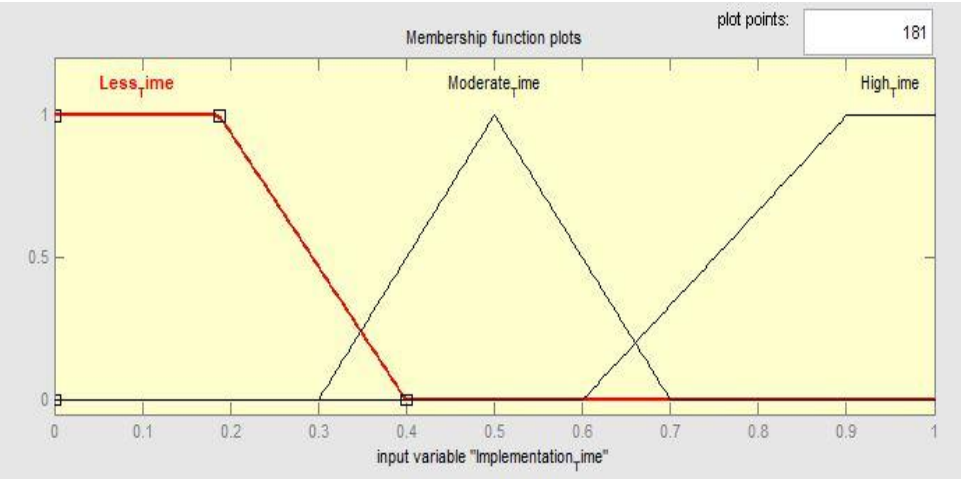


Figure 21. Linguistic Variables of Implementation Time for the Fuzzy Rates of Alternatives

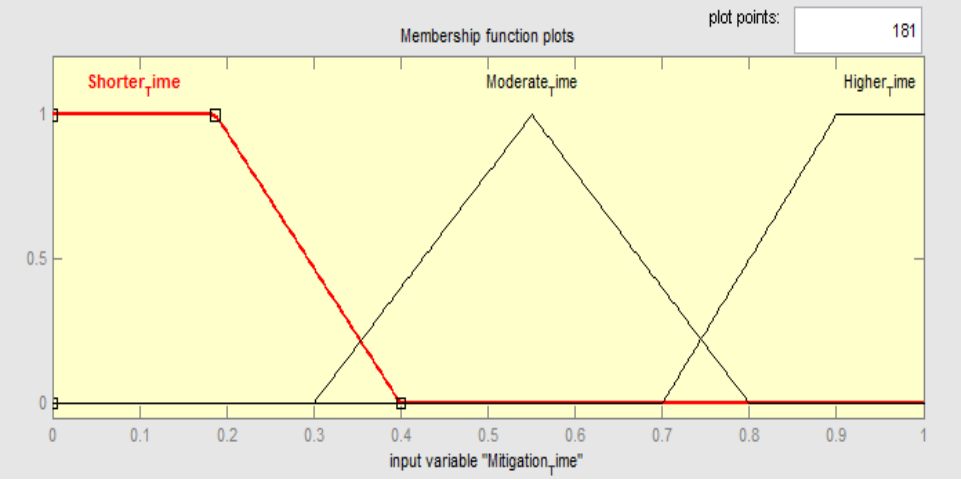


Figure 22. Linguistic Variables of Mitigation Time for the Fuzzy Rates of Alternatives

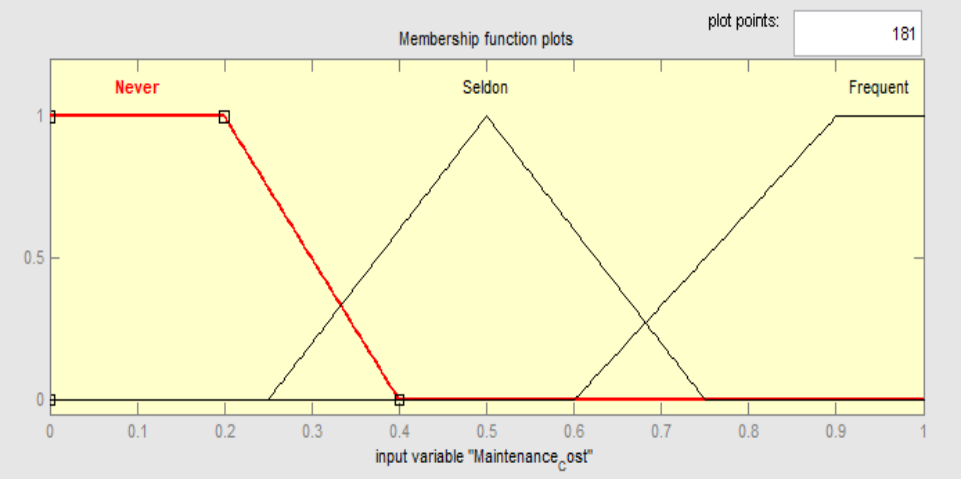


Figure 23. Linguistic Variables of Maintenance Cost for the Fuzzy Rates of Alternatives

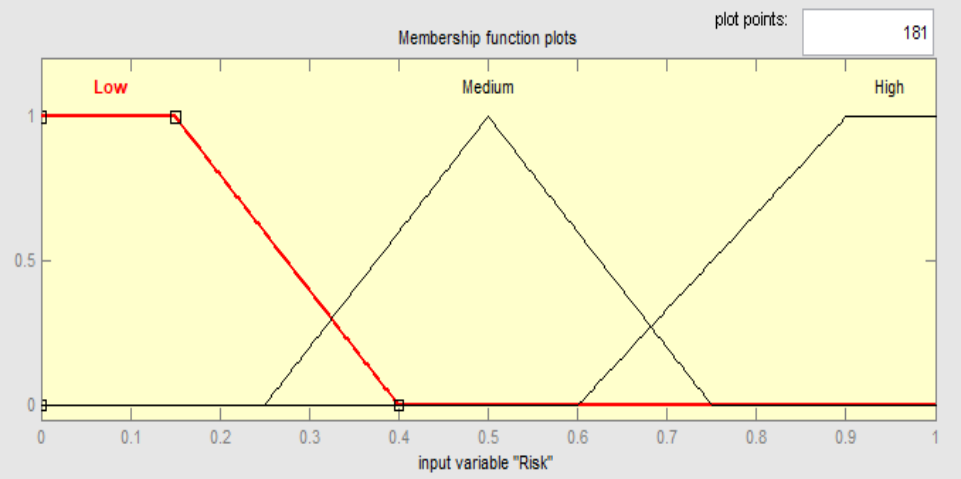


Figure 24. Linguistic Variables of Risk for the Fuzzy Rates of Alternatives

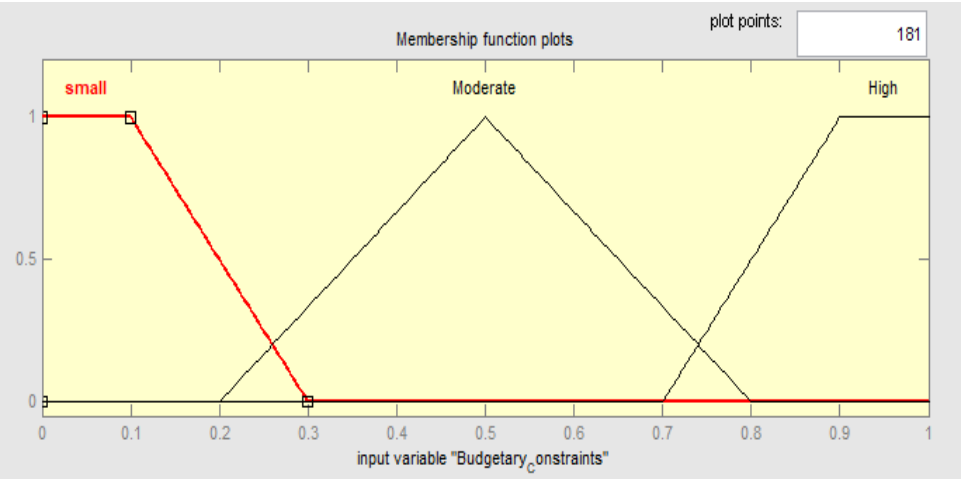


Figure 25. Linguistic variables of Budgetary Constraints for the Fuzzy Rates of Alternatives

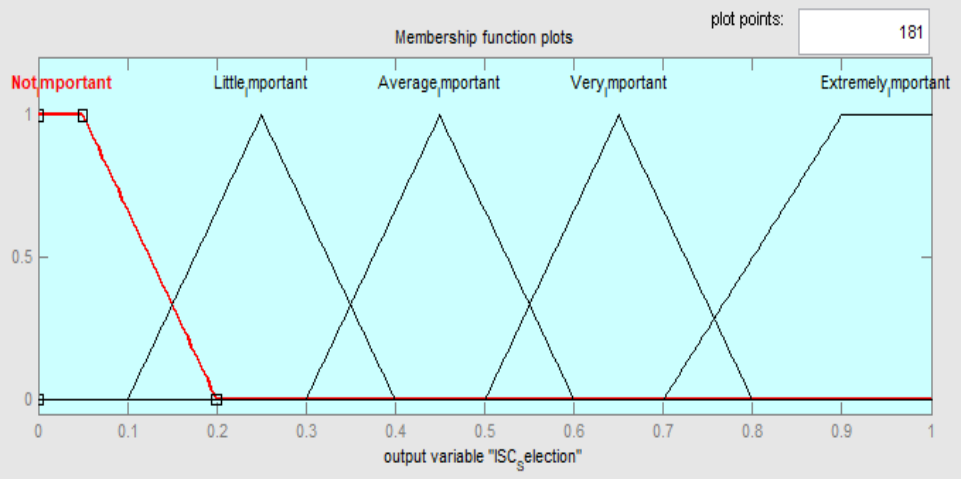


Figure 26. Linguistic Variables of ISC Selection for the Fuzzy Rates of Alternatives

The arithmetic and geometric operations were also applied to aggregate more than two TrFNs in this study.

There are several ways to aggregate two TrFNs. To aggregate more than two TrFNs, the existing technique was developed by [168] and it is also used in this proposed method. The following equations are used to aggregate two TrFNs.

$$a_{1_{ij}} = \min_{K}\{a_{1ij}^{k}\} \tag{2}$$

$$a_{2_{ij}} = \frac{1}{r}\sum_{k=1}^{r} e_{2_{ij}}^{k} \tag{3}$$

$$a_{3_{ij}} = \frac{1}{r}\sum_{k=1}^{r} e_{3_{ij}}^{k} \tag{4}$$

$$a_{4_{ij}} = \max_{K}\{a_{1ij}^{k}\} \tag{5}$$

After the aggregation of values, the output is still in fuzzy numbers. Therefore, it is necessary to conduct Defuzzification process to transform the fuzzy numbers into crisp numbers. The Defuzzification has many methods and in this study, the most used method center of areas (COA), the TrFN $\tilde{A}$ was defuzzified to crisp value ($C_{\tilde{A}}$). The Defuzzification formula is given as under:

$$C_{\tilde{A}} = \frac{a_3^2 + a_4^2 + a_3 a_4 - a_1^2 - a_2^2 - a_1 a_2}{3\,(a_3 + a_4 - a_1 - a_2)} \tag{6}$$

7.3.2 **Group Decision Making**

For a good decision, a combination of the view point / opinion or judgments of a number of decision makers is required as good decisions cannot be taken on the basis of arbitrary decisions of an individuals. Therefore, in this dissertation, for the sustainable selection of Information Security Controls, a method has been developed for the evaluation and selection process of Information Security Controls to get appropriate and sustainable results. The following elements are developed for group MCDM:

1. *m* possible Information Security Controls, A = {A_1, $A_2 \ldots A_m$}
2. *n* number of evaluation criteria for the selection of ISCs, C = {C_1, $C_2 \ldots C_n$};
3. K number of decision makers for the evaluation of ISCs, D = {D_1, $D_2 \ldots D_k$};

To develop a performance evaluation matrix of Information Security Controls, a decision matrix is required to be developed. The decision matrix of Information Security Controls using fuzzy linguistic assessment has following parameters:

1. Information Security Controls A_i = (*i*=1,2,…,*m*)
2. Criteria Cj = (*j*=1,2,…,*n*)
3. Decision Makers D_k (*k*=1,2,…,r)

$$E = \left[e_{ij}\right]_{n\times m} \qquad \begin{matrix} C_1 & \ldots\ldots\ldots & C_n \end{matrix}$$

$$= \begin{matrix} A_1 \\ \vdots \\ A_m \end{matrix} \begin{bmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{bmatrix}_{m\times n} \qquad i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n;\ k = 1, 2, \ldots r \qquad (7)$$

7.3.3 **Determination of Criteria Weightings**

Shannon [169] for the first time used the concepts of entropy in his research regarding information theory to measure the uncertainty. The entropy having smaller means higher criterion value means the greater criterion and greater role in the evaluation process and has the greater weight. The purpose of entropy weight is to deal with uncertainty and to deal with decision information that can be assigned to each evaluation criterion and thereafter relative weight of the criteria is obtained. In

relative weight calculation, no subjective factor is involved and it is calculated trough entropy weight method in which evaluation information of each alternative against evaluation criterion is used. In this method, the entropy weights are as under:

(1) The fuzzy decision evaluation matrix denoted by *E* (equation (7)) was defuzzified to crisp value matrix by:

$$E = \left[e_{ij}\right]_{n\times m} \rightarrow F = \left[f_{ij}\right]_{n\times m}$$

Where

$$\left[f_{ij}\right]_{n\times m} = \begin{array}{c} \\ A_1 \\ \vdots \\ A_m \end{array} \begin{array}{c} C_1 \ldots\ldots\ldots\ldots \\ \begin{bmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{m1} & \cdots & f_{mn} \end{bmatrix}_{m\times n} \end{array} \quad 1, 2, \ldots, m; j = 1, 2, \ldots, n; k = 1, 2, \ldots r \qquad (8)$$

(2) Construct normalized evaluation matrix

$$r_{ij} = \frac{f_{ij}}{\sqrt{\sum_{j=1}^{n} f_{ij}^2}} \qquad i = 1, 2, \ldots, m; j = 1, 2, \ldots, n \qquad (9)$$

(3) Develop weighted normalized decision matrix

$$V_{ij} = r_{ij} \times W_j \qquad i = 1, 2, \ldots, m; j = 1, 2, \ldots, n \qquad (10)$$

7.3.4 **Evaluation and Selection of Alternatives**

The TOPSIS method is the widely used method to get optimal solution through multiple-criteria decision making. The basic concept in the selection and evaluation of alternatives is to define positive ideal solution which has shortest distance and negative ideal solution that have longest distance. The positive ideal solution is called the best alternative against all evaluation criterions and vice versa. The defined alternatives are thereafter ranked by comparing the results against each alternative with the respect of their nearest positive ideal solution.

(1) The positive-ideal solution and negative-ideal solutions can be obtained as:

$$\begin{aligned} V_i^+ &= \left\{ \max_{1\le i\le n} \left(\left\{v_{ij}\right\}_{i=1}^{n} \right) | \, j \in J^+, \min_{1\le i\le n} \left(\left\{v_{ij}\right\}_{i=1}^{n} \right) \;\middle|\; j \in J_- \right\} \\ &= \left\{ v_{ij} \,\middle|\, j = 1,2 \ldots, n \right\} \end{aligned} \qquad (11)$$

$$V_i^- = \left\{ \min_{1 \le i \le n} \left(\{v_{ij}\}_{i=1}^n \right) | \, j \in J^+, \max_{1 \le i \le n} \left(\{v_{ij}\}_{i=1}^n \right) \, | j \, \in J_- \right\} = \{ v_{ij} \, | j = 1,2 \ldots, n \} \quad (12)$$

Where J^+ denoted as index set in which the greater value is better and J^- denoted as the index set where the smaller value is better.

(2) Next obtain the separation measure for each alternative. The separation from positive ideal solution S^+_i can be calculated as:

$$S_i^+ = \sqrt{\sum_{j=1}^{m} \left(V_{ij} - V_i^+ \right)^2} \quad , (i=1,2,\ldots,n) \quad (13)$$

Similarly, the separation of negative ideal solution S^-_i is calculated as:

$$S_i^- = \sqrt{\sum_{j=1}^{m} \left(V_{ij} - V_i^- \right)^2} \quad , (i=1,2,\ldots,n) \quad (14)$$

(3) To calculate the relative closeness to the ideal solution P_i^+

$$P_i = \frac{S_i^-}{S_i^+ + S_i^-} \quad (15)$$

7.4 STEP BY STEP CALCULATION

This section explained the comprehensive steps how this dissertation solved the main problem. The earlier the sections have already explained the types of Multi Criteria Decision Making (MCDM) methodologies, studied existing criteria and it's evaluated them to develop a comprehensive criteria for the assessment and evaluation of ISCs / alternatives, also explained the way to weight the alternatives and lastly calculation to complete Fuzzy TOPSIS, the MCDM method that was selected.

The proposed model in this dissertation have applied for Information Security Control section for Higher Education Institutions was consisted of the following steps:

Step 1: To construct the decision matrix by using linguistic variable, three decision makers were asked to rate the Information Security Controls with respect to each

criterion given in the Supplementary Material file. The Equation (7) was used to develop decision matrix.

Step 2: The next step was to convert the linguistic evaluations into trapezoidal fuzzy numbers.

Step 3: The rating of the decision makers was required to be aggregated. The Equation (2) (3) (4) and (5) was used to aggregate ranking of 3 decision makers and to construct the fuzzy decision matrix.

Step 4: The data derived from step 3 was defuzzified by Equation (6), the new decision matrix based on crisp values was developed by using Equation (8).

Step 5: The next step is to normalize the matrix by using Equation (9).

Step 6: The Equation (10) was used to determine the weight of the criterion.

Step 7: Calculates the positive ideal solution by using Equation (11) and negative ideal solution by using Equation (12).

Step 8: Calculates the distance of each alternative to the positive and negative ideal solution by using the Equation (13) and Equation (14) respectively.

Step 9: Calculates the relative proximity P_i by using Equation (15).

Step 10: The ISCs were ranked according to their relative proximityP_i .

7.5 FUZZY TOPSIS RESULTS

With Fuzzy TOPSIS complete, each Information Security Control received a score. The alternative received highest score is given rank 1; it means that ranked 1 control should be implemented 1st. The alternative that received lowest score is given lowest number and it should be implemented at the last. During calculating of the rank, it has been realized that ranks were not stable, means that as more decision maker's opinion were added, the rank was likely to change. To cater this issue, a preference band technique has been used to group similar scored alternatives together. The Table 15 shows the final results of ISCs including Fuzzy TOPSIS score, rank and preference band.

Table 15. Ranked Information Security Controls

Access Control Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference

AC-07	Unsuccessful Login Attempts	0.71682	Rank 1	Preference 1
AC-08	System Use Notification	0.71113	Rank 2	Preference 1
AC-05	Separation of Duties	0.65486	Rank 3	Preference 2
AC-09	Session Lock	0.65299	Rank 4	Preference 2
AC-06	Least Privilege	0.60053	Rank 5	Preference 2
AC-15	Publicly Accessible Content	0.53277	Rank 6	Preference 3
AC-04	Information Flow Enforcement	0.41874	Rank 7	Preference 4
AC-02	Account Management	0.40173	Rank 8	Preference 4
AC-10	Permitted Actions without Identification or Authentication	0.37731	Rank 9	Preference 5
AC-11	Remote Access	0.35344	Rank 10	Preference 5
AC-03	Access Enforcement	0.35083	Rank 11	Preference 5
AC-01	Access Control Policy and Procedures	0.33462	Rank 12	Preference 5
AC-13	Access Control for Mobile Devices	0.26957	Rank 13	Preference 6
AC-12	Wireless Access	0.22070	Rank 14	Preference 6
AC-14	User of External Information Systems	0.21335	Rank 15	Preference 6

Awareness and Training Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
AT-02	Awareness and Training Controls	0.89625	Rank 1	Preference 1
AT-01	Security Awareness and Training Policy and Procedures	0.73844	Rank 2	Preference 2
AT-04	Security Training Records	0.43734	Rank 3	Preference 3
AT-03	Role Based Security Training	0.22592	Rank 4	Preference 4

Audit and Accountability Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
AU-08	Protection of Audit Information	0.76023	Rank 1	Preference 1
AU-01	Audit & Accountability Controls	0.75009	Rank 2	Preference 1
AU-04	Audit Storage Capacity	0.73699	Rank 3	Preference 1
AU-07	Time Stamps	0.72731	Rank 4	Preference 1
AU-02	Audit Events	0.69350	Rank 5	Preference 2
AU-05	Response to Audit Processing Failures	0.61334	Rank 6	Preference 2
AU-03	Content of Audit Records	0.60102	Rank 7	Preference 2
AU-09	Audit Record Retention	0.56748	Rank 8	Preference 3
AU-06	Audit Review, Analysis, and Reporting	0.38404	Rank 9	Preference 4
AU-10	Audit Generation	0.35436	Rank 10	Preference 4

Contingency Planning Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
CM-02	Baseline Configuration	0.57791	Rank 1	Preference 1
CM-03	Security Impact Analysis	0.57294	Rank 2	Preference 1
CM-06	Software Usage Restrictions	0.53679	Rank 3	Preference 1
CM-04	Least Functionality	0.51760	Rank 4	Preference 1
CM-07	User Installed Software	0.45507	Rank 5	Preference 2
CM-01	Configuration Management Controls	0.45353	Rank 6	Preference 2
CM-05	Information System Component Inventory	0.34155	Rank 7	Preference 3

Contingency Planning Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
CP-03	Contingency Training	0.67686	Rank 1	Preference 1
CP-01	Contingency Planning Controls	0.61583	Rank 2	Preference 1
CP-04	Contingency Plan Testing	0.59207	Rank 3	Preference 2
CP-02	Contingency Plan	0.56959	Rank 4	Preference 2
CP-05	Information System Backup	0.35968	Rank 5	Preference 3
CP-06	Information System Recovery and Reconstitution	0.22978	Rank 6	Preference 4

Maintenance Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
MA-01	System Maintenance Policy and Procedures	0.57249	Rank 1	Preference 1
MA-04	Maintenance Personnel	0.55254	Rank 2	Preference 1
MA-02	Controlled Maintenance	0.54867	Rank 3	Preference 1
MA-03	Non-local Maintenance	0.45724	Rank 4	Preference 2

Media Protection Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
MP-03	Media Sanitization	0.62081	Rank 1	Preference 1
MP-02	Media Access	0.54153	Rank 2	Preference 2
MP-01	Media Protection Policy and Procedures	0.42587	Rank 3	Preference 3
MP-04	Media Use	0.42258	Rank 4	Preference 3

Planning Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
PL-01	Security Planning Policy and Procedures	1.00000	Rank 1	Preference 1
PL-02	System Security Plan	0.52854	Rank 2	Preference 2
PL-03	Rules of Behavior	0.18555	Rank 3	Preference 3

Risk Assessment Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
RA-01	Risk Assessment Policy and Procedures	0.64643	Rank 1	Preference 1
RA-03	Risk Assessment	0.56184	Rank 2	Preference 2
RA-04	Vulnerability Scanning	0.55820	Rank 3	Preference 2
RA-02	Security Categorization	0.12271	Rank 4	Preference 3

System and Services Acquisition Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
SA-04	External Information System Services	0.74631	Rank 1	Preference 1
SA-01	System and Services Acquisition Policy and Procedures	0.41945	Rank 2	Preference 2
SA-02	Allocation of Resources	0.39067	Rank 3	Preference 3
SA-03	System Development Life Cycle	0.36770	Rank 4	Preference 3

Identification and Authentication Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
IA-04	Authenticator Management	0.73576	Rank 1	Preference 1
IA-07	Identification and Authentication (Non-Institutional Users)	0.70008	Rank 2	Preference 1
IA-01	Identification and Authentication Policy and Procedures	0.48395	Rank 3	Preference 2
IA-02	Identification and Authentication (Organizational Users)	0.47445	Rank 4	Preference 2
IA-06	Cryptographic Module Authentication	0.35499	Rank 5	Preference 3
IA-03	Identifier Management	0.34888	Rank 6	Preference 3
IA-05	Authenticator Feedback	0.33942	Rank 7	Preference 3

Incident Response Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
IR-06	Incident Response Plan	0.54471	Rank 1	Preference 1
IR-05	Incident Response Assistance	0.50112	Rank 2	Preference 1
IR-01	Incident Response Policy and Procedures	0.50053	Rank 3	Preference 1
IR-04	Incident Monitoring	0.44582	Rank 4	Preference 2
IR-02	Incident Response Training	0.43159	Rank 5	Preference 2
IR-03	Incident Handling	0.28985	Rank 6	Preference 3

Personnel Security Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
PS-03	Personnel Screening	0.74282	Rank 1	Preference 1
PS-01	Personnel Security Policy and Procedures	0.64738	Rank 2	Preference 2
PS-06	Access Agreements	0.50787	Rank 3	Preference 3
PS-05	Personnel Transfer	0.48184	Rank 4	Preference 4
PS-07	Third-Party Personnel Security	0.47942	Rank 5	Preference 4
PS-02	Position Risk Designation	0.42071	Rank 6	Preference 4
PS-04	Personnel Termination	0.41135	Rank 7	Preference 4
PS-08	Personnel Sanctions	0.30531	Rank 8	Preference 5

System and Information Integrity Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
SI-05	Security Alerts, Advisories, and Directives	0.72626	Rank 1	Preference 1
SI-06	Information Handling and Retention	0.57122	Rank 2	Preference 2
SI-03	Malicious Code Protection	0.54485	Rank 3	Preference 2
SI-02	Flaw Remediation	0.41887	Rank 4	Preference 3
SI-04	Information System Monitoring	0.36122	Rank 5	Preference 4

Physical and Environmental Protection Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
PE-02	Physical Access Authorizations	0.64725	Rank 1	Preference 1
PE-03	Physical Access Control	0.62832	Rank 2	Preference 1
PE-06	Emergency Lighting	0.57983	Rank 3	Preference 2
PE-08	Temperature and Humidity Controls	0.53726	Rank 4	Preference 2
PE-01	Physical and Environmental Protection Policy and Procedures	0.49227	Rank 5	Preference 3
PE-05	Visitor Access Records	0.47066	Rank 6	Preference 3
PE-04	Monitoring Physical Access	0.43188	Rank 7	Preference 3
PE-10	Delivery and Removal	0.39743	Rank 8	Preference 4
PE-09	Water Damage Protection	0.30376	Rank 9	Preference 4
PE-07	Fire Protection	0.26447	Rank 10	Preference 5

Program Management Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
PM-08	Threat Awareness Program	0.79210	Rank 1	Preference 1
PM-05	Information System Inventory	0.74793	Rank 2	Preference 1
PM-02	Information Security Officer	0.69051	Rank 3	Preference 2
PM-01	Program Management Policy and Procedures	0.55718	Rank 4	Preference 3
PM-06	Information Security Measures of Performance	0.50864	Rank 5	Preference 3
PM-04	Plan of Action and Milestones Processes	0.49157	Rank 6	Preference 4
PM-03	Information Security Resources	0.45372	Rank 7	Preference 4
PM-07	Enterprise Architecture	0.32970	Rank 8	Preference 5

Security Assessment and Authorization Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
CA-07	Internal System Connections	0.71181	Rank 1	Preference 1
CA-02	Security Assessments	0.67491	Rank 2	Preference 2
CA-06	Continuous Monitoring	0.63224	Rank 3	Preference 2
CA-05	Security Authorization	0.57395	Rank 4	Preference 3
CA-04	Plan of Action and Milestones	0.29982	Rank 5	Preference 4
CA-03	Information System Connections	0.29799	Rank 6	Preference 4
CA-01	Security Assessment and Authorization Policies and Procedures	0.19203	Rank 7	Preference 5

System and Communications Protection Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
SC-06	Collaborative Computing Devices	0.66564	Rank 1	Preference 1
SC-05	Cryptographic Protection	0.63262	Rank 2	Preference 1
SC-04	Cryptographic Key Establishment and Management	0.62277	Rank 3	Preference 1
SC-07	Process Isolation	0.50637	Rank 4	Preference 2
SC-01	System and Communications Protection Policy and Procedures	0.39418	Rank 5	Preference 3
SC-02	Denial of Service Protection	0.37867	Rank 6	Preference 3

SC-03	Boundary Protection	0.33451	Rank 7	Preference 3

Mobile Security Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
MS-15	Passwords	0.66178	Rank 1	Preference 1
MS-03	Application Stores	0.65156	Rank 2	Preference 1
MS-17	Security Patches	0.63583	Rank 3	Preference 1
MS-09	Device Eligibility	0.62863	Rank 4	Preference 1
MS-02	Anti-Malware	0.62582	Rank 5	Preference 1
MS-05	Approved Software for BYOD	0.61143	Rank 6	Preference 1
MS-16	Backup Policy	0.57736	Rank 7	Preference 2
MS-12	Encryption	0.57498	Rank 8	Preference 2
MS-04	Approved Applications and Stores	0.55898	Rank 9	Preference 2
MS-11	Device Management	0.52549	Rank 10	Preference 2
MS-10	Device Inventory	0.49468	Rank 11	Preference 3
MS-07	Cloud Based Services	0.47947	Rank 12	Preference 3
MS-06	Mobile Awareness and Training	0.45897	Rank 13	Preference 3
MS-14	Lockout Screen	0.44648	Rank 14	Preference 3
MS-08	Compatibility	0.42470	Rank 15	Preference 3
MS-01	Mobile Security Policy and Procedure	0.42218	Rank 16	Preference 3
MS-13	Jailbreaking and Rooting	0.35198	Rank 17	Preference 4

Infrastructure & Virtualization Security Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
IV-03	Change Detection	0.72738	Rank 1	Preference 1
IV-10	Segmentation	0.70348	Rank 2	Preference 1
IV-07	Network Security	0.65639	Rank 3	Preference 2
IV-04	Clock Synchronization	0.59489	Rank 4	Preference 3
IV-02	Audit Logging / Intrusion Detection	0.57079	Rank 5	Preference 3
IV-06	Vulnerability Management	0.56318	Rank 6	Preference 3
IV-08	OS Hardening and Base Controls	0.52622	Rank 7	Preference 3
IV-09	Separation of Environment	0.50250	Rank 8	Preference 3
IV-13	Network Architecture	0.42478	Rank 9	Preference 4
IV-05	Information System Documentation	0.42295	Rank 10	Preference 4
IV-12	Hypervisor Hardening	0.41420	Rank 11	Preference 4
IV-01	Infrastructure & Virtualization Security Policy and Procedure	0.27074	Rank 12	Preference 5
IV-11	VM Security - Data Protection	0.26371	Rank 13	Preference 5

Interoperability & Portability Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
IP-01	Interoperability & Portability	0.58344	Rank 1	Preference 1
IP-04	Standardized Network Protocols	0.51067	Rank 2	Preference 1
IP-03	Data Request	0.47938	Rank 3	Preference 2
IP-02	APIs	0.41949	Rank 4	Preference 2
IP-05	Virtualization	0.40792	Rank 5	Preference 2

Business Continuity Management & Operational Resilience Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
BC-03	Business Continuity Testing	0.69609	Rank 1	Preference 1
BC-06	Impact Analysis	0.69166	Rank 2	Preference 1
BC-02	Business Continuity Planning	0.62182	Rank 3	Preference 1
BC-04	Datacentre Utilities / Environmental Conditions	0.62089	Rank 4	Preference 1
BC-05	Equipment Location and Maintenance	0.60261	Rank 5	Preference 1
BC-01	Business Continuity Management & Operational Reliance	0.51118	Rank 6	Preference 2
BC-07	Retention Policy	0.42734	Rank 7	Preference 3

Data Security & Information Life-Cycle Management Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
DS-05	Ownership / Stewardship	0.70558	Rank 1	Preference 1
DS-02	Classification	0.69194	Rank 2	Preference 2
DS-04	Handling / Labelling / Security Policy	0.53217	Rank 3	Preference 3
DS-03	Ecommerce Transactions	0.36882	Rank 4	Preference 4
DS-01	Data Security & Information Life-Cycle Management Policy & Procedures	0.20146	Rank 5	Preference 5

Supply Chain Management, Transparency, and Accountability Family Controls

Controls Number	Control	Fuzzy TOPSIS Score	Rank	Preference
SM-08	Third Party Audits	0.67958	Rank 1	Preference 1
SM-03	Network and Infrastructure Services	0.65699	Rank 2	Preference 1
SM-06	Supply Chain Governance Reviews	0.59165	Rank 3	Preference 2
SM-05	Supply Chain Agreements	0.54785	Rank 4	Preference 2
SM-04	Institute Internal Assessments	0.46652	Rank 5	Preference 3
SM-01	Data Quality and Integrity	0.40757	Rank 6	Preference 3
SM-07	Third Party Assessment	0.31427	Rank 7	Preference 4
SM-02	Incident Reporting	0.30365	Rank 8	Preference 4

The given above controls have different ranks but fall under the same preference band as another controls, there is a no big difference and they are considered equal. It should be stressed that all security checks of the first preference band should be implemented before moving on to the second and to the following preference bands. After the calculation of the results, it is important to validate the stability of the results. This task was accomplished through sensitivity analysis.

7.6 DATA ANALYSIS

After calculating Fuzzy TOPSIS's results, it is necessary to execute sensitivity analysis to check the stability of the results and judge imprecise input. In MCDM problem, the results may imprecise and changeable. Therefore, it is important to

perform sensitivity analysis on the input data. It is an important step in many applications of MCDM which is to perform a sensitivity analysis on the input data. The sensitivity analysis is a technique to validate the expert's opinion and effect of the minor changes of input on results.

There are basically two types of sensitivity analysis. One in which more survey is added to check the change in the result. Second, perform sensitivity analysis is performed by increasing and decreasing weights of each criteria. The second test is very essential to perform, if after changing the weights of the criteria and there is no change or minor change in the results, then the results may be selected. Therefore, performed only second test on the Access Control family as a sample was performed.

7.6.1 **Sensitivity Analysis – Varying Weight**

Sensitivity analysis is a way to know how much uncertainty in the output of a model due to uncertainty in the input of the model. Each criteria of the MCDN has assigned weight. It is required to check whether a slight change in the weight has a large impact on the output or not? If there is slightly variation in the output then it is obvious; however, if a large change occurs in the output due to minor change in the input, then this is an issue with model.

In Sensitivity analysis, analyse each of six weights of criteria is analysed individually by increasing the weight of the criteria from 1% to 5%. In this analysis, the weight up to 10% will be increased to see the impact on result.

7.6.2 **Effectiveness**

During above said analysis, the weight of the effectiveness criteria was found varied. The initial value of the weight 0.2, as researcher increased its weight to 0.21, it was observed that only one control i.e. AC-06 changed its preference band from 02 to 03. Then increased the weight to 0.22 was increased, only two controls AC-03 and AC-13 preference band were changed and the same controls were effected when the weight to 0.23 was increased. Similarly, at 0.24 weight, the preference band of AC-06, AC-03 and AC-13 were changed. At weight 0.24, the preference band of AC-07, AC-08, AC-04 and AC-13 were up and down. The sensitivity of the weights was also increased by increasing it at 10% (0.3), and observed that preference band of 08 controls were change. Figure 27 illustrates these results.

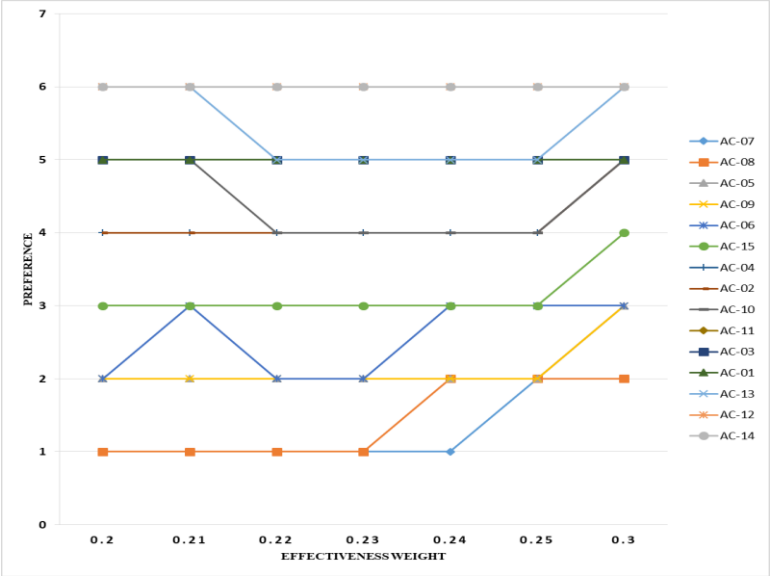


Figure 27. Analysis of Preference and Effectiveness weights

7.6.3 **Implementation Time**

To better analysis of the results, the weight was required to be increased by 0.1. There was no change in the weights from 0.15 to 2.0 whereas preference band of the only two controls (AC-10 and AC-13) were changed 10% (0.25) was increased. Analysis shows that there is no change in the preference band when varying the weight of the implementation time. The Figure 28 presents the results.

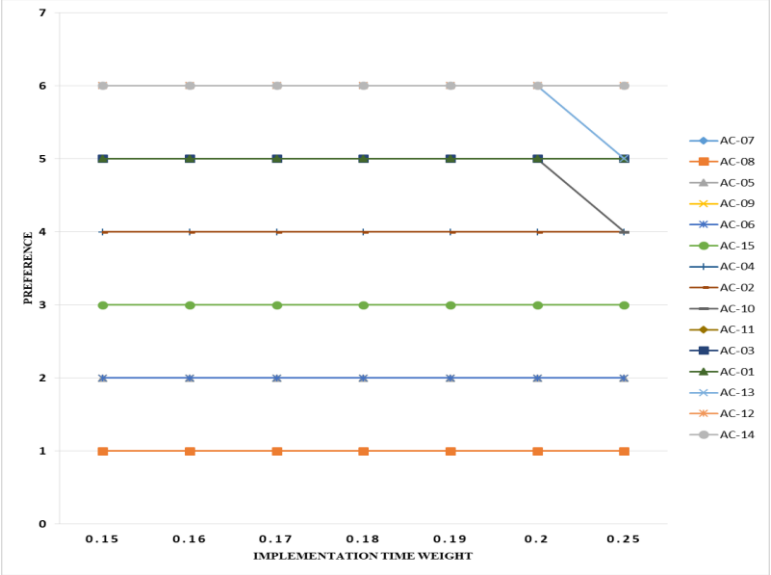


Figure 28. Analysis of Preference and Implementation Time weights

7.6.4 **Mitigation Time**

The initial weight value set for mitigation time is also 0.15. The weight of the mitigation time criteria was varied from 0.15 to 0.20 but there is no change in the

preference band of the controls. When its value from 0.15 to 0.25 was changed, then preference band of the AC-01 and AC-10 were changed. Hence, varying the weight of the criteria has very minor impact of the criteria. The Figure 29 clearly shows the results.

7.6.5 **Maintenance Time**

The maintenance time has also very minor impact on the results. The weight of the maintenance time criteria from 0.15 to 0.20 was varied but only one control AC-02 preference band was changed. When its value from 0.15 to 0.25 was changed, then preference band of the AC-02 and AC-04 were changed. Hence, varying the weight of the maintenance time criteria has also very minor impact. The Figure 30 clearly depicts the results.

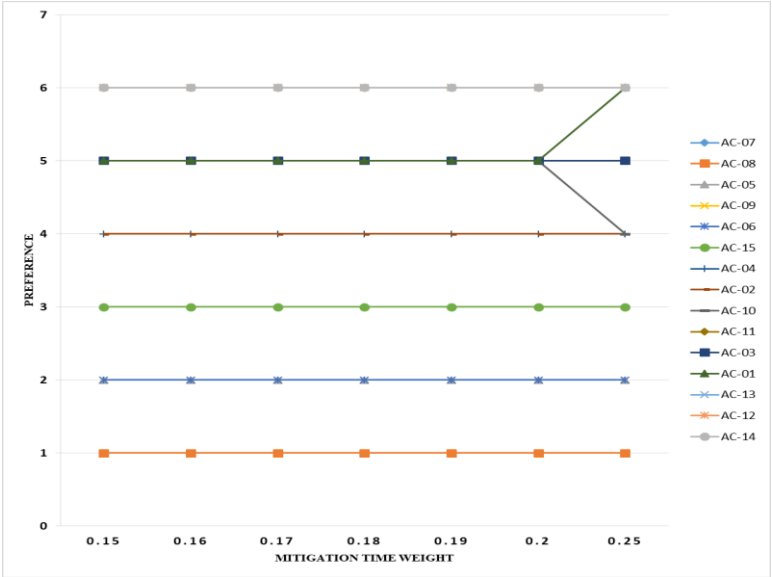


Figure 29. Analysis of Preference and Mitigation Time weights

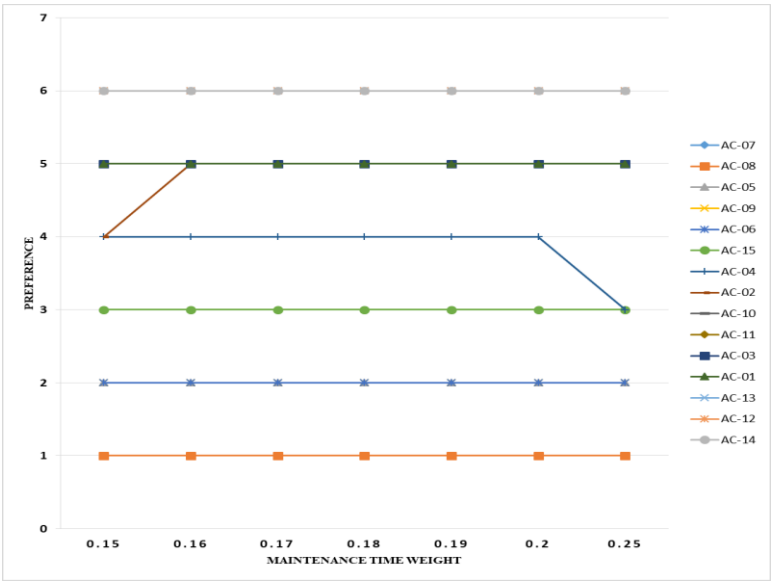


Figure 30. Analysis of Preference and Maintenance Time weights

7.6.6 **Risk**

The Figure 31 shows that there is not much change in the results after varying the weights. The weight of the Risk criteria was increased from 0.1 to 0.15 even checked 0.2 and it was found that there is very minor change in the already determined preference of the alternative. Figure 31 demonstrates preference versus Risk criteria results graphically.

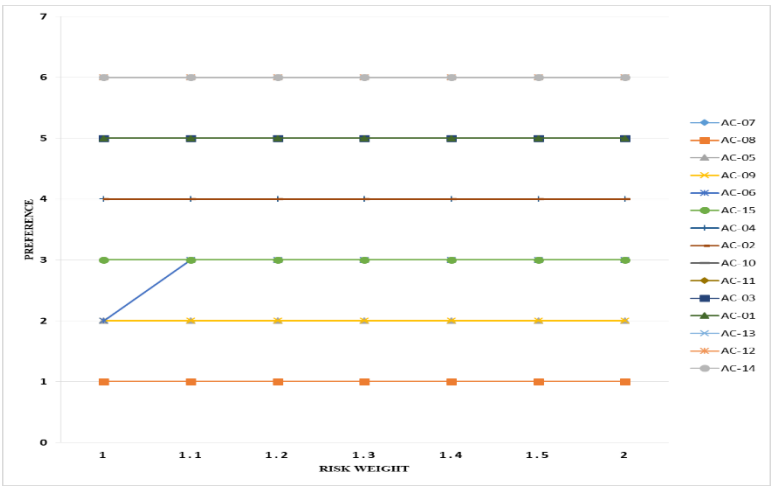


Figure 31. Analysis of Preference and Risk criteria weights

7.6.7 **Budgetary Constraints**

The weight of the Budgetary Constraints was increased and it was found that there is very minor change in the already determined preference of the alternative. It was observed that there was no change in the preference from 0.25 to 0.28. At Budgetary Constraint weight value 0.29, only AC-14 preference band changed from 06 to 07

and then at point 0.30, the same results i.e. change of AC-14 preference band from 06 to 07. But increased the said weight from .25 to .35 was increased, the preference band of 4 alternatives (AC-05, AC-10, AC-01 and AC-14) were one step down in preference. The analysis shows that majority of the alternatives retained their preference band. Figure 32 demonstrates preference versus Budgetary Constraints results graphically.

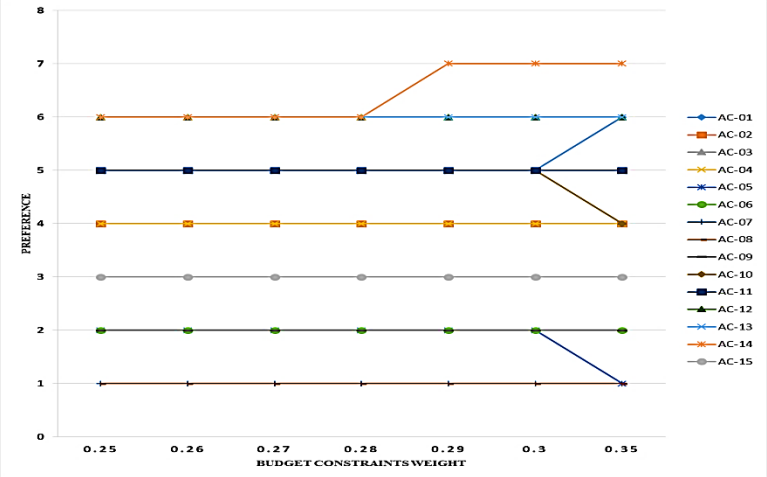


Figure 32. Analysis of Preference and Budgetary Constraints weights

Chapter 8: Conclusion and Future Work

This chapter contains the ending of the research work. It has been summarized in the form of main findings and contributions. Furthermore, some limitations and future research are also given at the end of this chapter. In addition, research publications by the researcher originated from this work have also been mentioned.

8.1 RESEARCH OVERVIEW

Cloud computing technology is a comparative new technology in information technology field and many large educational institutions with large IT infrastructure and systems have not been able to get the benefits of Cloud Computing because of many technological, environmental, security, cultural and organizational constraints. These problems must be resolved through examining the challenges of cloud computing adoption in Higher Educational Institutions. One of the key problems faced by large Higher Education Institutions is the spending of large amounts in IT infrastructure but it still faces security and privacy issues. The future of Higher Education Institutions lies in cloud computing technology, where the main goal is to reduce IT cost, secure IT infrastructure and information system while increasing productivity, reliability, elasticity, and reduced secured response times. With the aid of secured cloud computing, Higher Education Institutions can focus more on their goals of education, which is useful for all types of education.

The first focus of the thesis is detailed investigation to help Higher Education Institutions to understand why they are not adopting cloud computing and guide them about enhanced and more efficient cloud adoption. There has been no research to study the factors that influence the adaption of Higher Education Institutions. The current study aims to provide a better understanding of the nature of the problems and provides practical evidence that may lead to the adoption of cloud computing in the near future in the Higher Education Institutions of Pakistan.

The study used a multiple approach to include several types of Higher Education Institutions of Pakistan. The research was conducted in stages to gather the required data, and quantitative methods were used to enrich and improve the quality and variety of the collected data.

Securely connection with external systems in the virtual world is a key element in a supportive as well as healthy leaning and teaching environment. This is mainly the case in Higher Education Institutions of Pakistan, where students and scholars are progressively learning in digital formats; even teachers, staff, and visitors of the Institutions are sharing their information and notes online even then manage their infrastructure and facilities online. To uphold their joint culture, Higher Education Institutions and universities have strong IT networks and multi-level infrastructure systems with different levels of access and connectively. Regrettably, this open information system has made Higher Education Institutions around the world targeted in cyber-attacks in 2017. Higher Education Institutions are not first and new targets for cyber-attacks and malicious codes. Literature review revealed that that during the years 2005 to 2014, too much data gaps were reported in numerous Higher Education Institutions. Hacking of systems and unintentional disclosure of information were the examples reported within HEIs. When an Institutions is threatened off with an online attack or risk, the impact goes beyond the loss of personal and secret information of the students and staff. There may be operational and financial implications, as well as security and privacy issues, as some Higher Education Institutions participate in research projects for military. This is core reason to develop secured Hybrid Cloud Information Security Framework particularly for the Higher Education Institutions to protect the integrity, privacy and confidentiality of the information / data of the staff and students.

The Heads of the Higher Education Institutions struggle how to manage and understand efficiently about the challenges and problems associated with information security. These Heads of the Institutions take interest to know how other Higher Education Institutions are managing information security in their institutions and tackling the challenges. It is essential to have operational support to achieve the goals and objectives of information privacy and security. By implementing the proposed framework of the thesis that maintains ongoing information about security and privacy issues, the Heads of the Higher Education Institutions can give assurances to their staff members and students that their Institutions are adopting relevant effective methods and techniques for the security of their information system.

The following given below brief overviews about each chapter of this thesis are:

Chapter 1, the research problem was clearly elaborated and the importance of this study was also explained thoroughly. In addition, research questions, goals and objectives were clearly mentioned. Finally, the chapter explained the structure of the thesis.

Chapter 2, discusses about the findings extracted during literature review and identifies the factors that influence the adoption of cloud computing in Higher Education Institutions of the Punjab, Pakistan. The gap between identified knowledge and the research work is also highlighted. In addition, the theoretical background of the research problem has also been discussed in the light of previous studies.

Chapter 3, provides a literature review to establish an appropriate conceptual framework that follows TOE and Diffusion of Innovation framework. This thing guided to develop a conceptual model for the adoption of cloud computing in Higher Education Institutions of Punjab, Pakistan. The theoretical basis of the model was studied in depth, and the hypotheses of this conceptual framework was also discussed in detail.

Chapter 4, discusses about the selected methods for research, and how the goals and objectives of the present research were achieved with the support of selected methods and approaches. Furthermore, it also explained about the data collection mechanism and analysis. The justification of the adopted methods, and techniques are also analysed.

Chapter 5, presents and provides the analysis of quantitative data obtained from the questionnaire. This chapter also provided all statistical results of the pilot survey. The Results of the empirical study were categorized against each factor influencing on the adoption of cloud computing in Higher Education Institutions. The purpose of this chapter was to determine the statistical significance of each identified factor. Different quantitative techniques of analysis were adopted. The statistical model was developed to test the hypothesis like T-Test and Regression Analysis etc.

Chapter 6, the solution identified and it was proposed How Hybrid Cloud framework can be secured for Higher Education Institutions in Pakistan. In this chapter, initially the principles of the framework were explained, which became evident from the material discussed in this thesis. Later, the framework was presented along with a detailed discussion of its twenty four modules including

information security controls for fine working. In addition, the core benefits of the framework were highlighted. It has also been identified that these benefits can be applied for improvements in the information security of the Institutions.

Chapter 7, Large Higher Education Institutions has required a large amount of resources to protect their information and Institute assets. In the preceding chapter, large frameworks have been created in order to guide them effectively about the processes that are required for security. Higher Education Institutions neither have sufficient resources nor absolute expertise to meet information security standards as the large number of Higher Education Universities do. The frameworks that giant Universities rely on are infeasible for Higher Education Institutions in an efficiently way. In the proposed framework, a large number of information security controls have also been proposed and it is very hard for the administration of the Institutions to explain or justify their recommendations about the implementations of the information security controls. To cater this issue, this chapter presented Fuzzy based Multi Criteria Decision Making which is opted by other cyber security experts. This chapter demonstrated this methodology by prioritizing the proposed information security controls which are applicable to Higher Education Institutions.

8.2 RESEARCH CONTRIBUTION

This study is distinct in its nature as no investigation has been conducted in respect of Higher Education Institutions of Punjab, Pakistan. The cloud computing users of the Higher Education Institutions were approached in each division of the Punjab, which is a major achievement. The authorities of these Institutions encouraged the researcher by granting access to these Institutions, because they considered the research will be very fruitful for their Institutions. As explained above, the Higher Education Institutions in Punjab, Pakistan have specific characteristics, and, therefore, it was necessary to understand their problems from their point of view, as other standard solutions and recommendations cannot work there.

The main contributions of this thesis are as under:

Contribution 1: A comprehensive literature survey was conducted to identify the factors that affect the adoption of the cloud computing in Higher Education Institutions in the Punjab, Pakistan. This comprehensive review enabled to include 34 factors for investigation.

Contribution 2: The deficiencies in the existing theoretical models were identified that are being used to understand the challenges which affect the adoption of cloud computing and on the basis of these deficiencies, a comprehensive theoretical model was developed specifically for this study. In the light of this theoretical model, survey questionnaire method was used. The proposed conceptual model was analyzed and tested in Chapters 5.

Contribution 3: The existing renowned information security standards i.e. NIST, ISO/IEC and Cloud Control Matrix have been analyzed by developing different criteria to get the effectiveness of the controls of the frameworks for Cloud Computing. The results of the evaluation have been given in the Chapter 6.

Contribution 4: Introduced Agent Based threat management framework for hybrid cloud computing and Agent based information Security framework duly simulated through fuzzy logic. These frameworks will help Higher Education Institutions to tackle Institutional threats and manage the security of the Institutes through multiple agents.

Contribution 5: No information security framework is existed particularly for the Higher Education Institutions of Punjab, Pakistan to meet their security requirements. To protect the Higher Education Institutions, a low cost, effective and secured information security framework for hybrid cloud computing has been proposed that have in 24 domains and in chapter 6, each module is explained in detail. For effective implementation of the framework, cost effective information security controls were also developed in the framework that the researcher deems it's essential for each Institution.

Contribution 6: The proposed framework was compared with the other renowned information security frameworks that are used in the Higher Education Institutions to get its better effectiveness for the Higher Education Institutions. The proposed framework is also validated in the light of the information security principles and extracted that the proposed framework is fulling the requirements of the reliability of the information security framework. Finally, the author conducted risks based analysis of the proposed framework by identifying cloud based information security risks and threats and mapped these risks to proposed information security controls to demonstrate that the proposed framework and it's IS controls has the capability to mitigate these risks.

Contribution 7: Although there are various techniques to validate and prioritize the information security controls but the researcher used combination of Fuzzy based Multi Criteria Decision Making and TOPSIS techniques to validate the authenticity of the proposed information security controls. Fuzzy TOPSIS combination provides more accurate results as compared to the other techniques which have been discussed in this chapter.

Contribution 8: Developed an Agent Based Information Security Framework that secures organizations from potential risks and threats. Then it introduces Agent technique in Information Security Risk Assessment to mitigate the risks effectively and remove threats. It compared the proposed framework with existing seven renowned Risk Assessment methods to validate its novelty. Moreover, ABISF was evaluated by using fuzzy logic simulation techniques to validate its effectiveness.

8.3 SUGGESTIONS FOR FUTURE RESEARCH

The development of the secured hybrid cloud computing information security framework relied upon on the basis of the cloud adoption constraints, current security issues in Higher Education Institutions and the information security requirements of the Higher Education Institutions of Punjab, Pakistan. In future, more researches will be conducted to develop information security framework for other provinces of Pakistan. It will also meet education industry requirements.

The research cite of this work was Higher Education Institutions. The research could be conducted to expand this framework for the use by Higher Education Universities. Although, a few off-the-shelf information security frameworks exist to assist HEIs, but a simplified, and cost effective, practically applicable comprehensive solution may be operated in an efficient way.

During literature review and the development of the information security framework, the researcher could not find a single set of procedures and methods to implement information security controls in Higher Education Institutions. Thus, the research was conducted to develop a set of comprehensive procedures and methods to implement information security controls. Accordingly, this might be highly helpful for future information security implementations.

The audit of the information security controls in the organization is essentially required to know how much operational team is adhered to the information security

controls. Therefore, in future, more research will be conducted by handing over questionnaire to the operational staff and technical staff of the Higher Education Institutions to evaluate their adherence as well as effectiveness of the security procedures in the context of security controls. The responses of both the staff on the questionnaires will be very beneficial to get a more unprejudiced view of information security control compliance.

Bibliography

[1] M. I. Tariq, "Towards information security metrics framework for cloud computing," *International Journal of Cloud Computing and Services Science*, vol. 1, no. 4, p. 209, 2012.

[2] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," presented at the Proceedings of the 2015 workshop on mobile big data, 2015, pp. 37–42.

[3] D. Puthal, B. Sahoo, S. Mishra, and S. Swain, "Cloud computing features, issues, and challenges: a big picture," presented at the Computational Intelligence and Networks (CINE), 2015 International Conference on, 2015, pp. 116–123.

[4] M. I. Tariq and V. Santarcangelo, "Analysis of ISO 27001: 2013 Controls Effectiveness for Cloud Computing.," presented at the ICISSP, 2016, pp. 201–208.

[5] Muhammad Imran Tariq, "Analysis of the Effectiveness of Cloud Control Matrix for Hybrid Cloud Computing," *International Journal of Future Generation Communication and Networking*, vol. 11, no. 4, pp. 1–20, 2018.

[6] M. I. Tariq, S. Tayyaba, M. W. Ashraf, H. Rasheed, and F. Khan, "Analysis of NIST SP 800-53 Rev. 3 Controls Effectiveness for Cloud Computing," *computing*, vol. 3, p. 4, 2017.

[7] A. R. Otero, "An Information Security Control Assessment Methodology for Organizations," p. 176, 2014.

[8] S. Jain, "A trust model in cloud computing based on fuzzy logic," presented at the Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on, 2016, pp. 47–52.

[9] R. Alguliyev and F. Abdullayeva, "Development of Fuzzy Risk Calculation Method for a Dynamic Federation of Clouds," *Intelligent Information Management*, vol. 7, no. 04, p. 230, 2015.

[10] L. Zhao, "Evaluation and Analysis on Security Framework Model of Cloud Computing," in *Proceedings of the 2015 4th International Conference on Computer, Mechatronics, Control and Electronic Engineering*, Guangzhou, China, 2015.

[11] A. Sharma and H. Banati, "A framework for implementing trust in cloud computing," presented at the Proceedings of the International Conference on Internet of things and Cloud Computing, 2016, p. 6.

[12] S. Kumar, S. Mittal, and M. Singh, "Fuzzy based trust management system for cloud environment," *Advances in Science and Technology Research Journal*, vol. 10, no. 30, pp. 32–37, 2016.

[13] S. Gupta and A. K. Saini, "Modeling Trust Based Risk Management in Cloud Adoption using Fuzzy Inference System," *International Journal of Technology Diffusion (IJTD)*, vol. 8, no. 1, pp. 52–60, 2017.

[14] A. Selvaraj and S. Sundararajan, "Evidence-based trust evaluation system for cloud services using fuzzy logic," *International Journal of Fuzzy Systems*, vol. 19, no. 2, pp. 329–337, 2017.

[15] H. M. Sabi, F.-M. E. Uzoka, K. Langmia, and F. N. Njeh, "Conceptualizing a model for adoption of cloud computing in education," *International Journal of Information Management*, vol. 36, no. 2, pp. 183–191, 2016.

[16] M. I. Tariq, "Providing Assurance to Cloud Computing through ISO 27001 Certification: How Much Cloud is Secured After Implementing Information Security Standards," 2015.

[17] S. Aljawarneh, *Cloud computing advancements in design, implementation, and technologies*. IGI Global, 2012.

[18] T. Ercan, "Effective use of cloud computing in educational institutions," *Procedia-Social and Behavioral Sciences*, vol. 2, no. 2, pp. 938–942, 2010.

[19] M. Zhanikeev, "A Cloud Visitation Platform to Facilitate Cloud Federation and Fog Computing.," *IEEE Computer*, vol. 48, no. 5, pp. 80–83, 2015.

[20] K. Manjula and P. Karthikeyan, "Cloud Computing–A Paradigm Shift," *Global Journal of Computer Science and Technology*, 2010.

[21] S. Chakraborty and K. Roy, "An SLA-based framework for estimating trustworthiness of a cloud," presented at the Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012, pp. 937–942.

[22] E. Siougle and V. Zorkadis, "A model enabling law compliant privacy protection through the selection and evaluation of appropriate security controls," in *Infrastructure Security*, Springer, 2002, pp. 104–114.

[23] ISACA., *COBIT 5: A business framework for the governance and management of enterprise IT*. Isaca, 2012.

[24] L. ISO, "IEC 27001: 2013," *Information technology–Security techniques–Information security management systems–Requirements*, 2013.

[25] S. Saxena, "Ensuring cloud security using cloud control matrix," *International Journal of Information and Computation Technology*, pp. 933–938, 2013.

[26] Y. L. Yang and Y. H. Zhou, "A Fuzzy Logic Based Information Security Risk Assessment Method," presented at the Applied Mechanics and Materials, 2012, vol. 130, pp. 3726–3730.

[27] Y. Yang and Y. Zhou, “Fuzzy logic based method for network information security risk assessment,” presented at the Internet Technology and Applications (iTAP), 2011 International Conference on, 2011, pp. 1–4.
[28] S.-T. Lu and S.-H. Yu, “Risk Factors Assessment for Software DevelopmentProject Based on Fuzzy Decision Making,” *International Journal of Information and Electronics Engineering*, vol. 2, no. 4, p. 596, 2012.
[29] A. M. Ortiz and T. Olivares, “Fuzzy logic applied to decision making in wireless sensor networks,” in *Fuzzy Logic-Emerging Technologies and Applications*, InTech, 2012.
[30] M. Fayaz, I. Ullah, D.-H. Park, K. Kim, and D. Kim, “An integrated risk index model based on hierarchical fuzzy logic for underground risk assessment,” *Applied Sciences*, vol. 7, no. 10, p. 1037, 2017.
[31] I. Anikin and L. Y. Emaletdinova, “Information security risk management in computer networks based on fuzzy logic and cost/benefit ratio estimation,” presented at the Proceedings of the 8th International Conference on Security of Information and Networks, 2015, pp. 8–11.
[32] N. Pilevari, A. Toloei, and M. Sanaei, “A model for evaluating cloud-computing users satisfaction,” *African Journal of Business Management*, vol. 7, no. 16, pp. 1405–1413, 2013.
[33] M. Jouini and L. B. A. Rabai, “A Security Framework for Secure Cloud Computing Environments:,” *International Journal of Cloud Applications and Computing*, vol. 6, no. 3, pp. 32–44, Jul. 2016.
[34] L. Barnard and R. Von Solms, “A formalized approach to the effective selection and evaluation of information security controls,” *Computers & Security*, vol. 19, no. 2, pp. 185–194, 2000.
[35] H. Gatignon and T. S. Robertson, “Technology Diffusion: An Empirical Test of Competitive Effects,” *Journal of Marketing*, vol. 53, no. 1, pp. 35–49, 1989.
[36] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, “User Acceptance of Computer Technology: A Comparison of Two Theoretical Models,” *Management Science*, vol. 35, no. 8, pp. 982–1003, Aug. 1989.
[37] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “User Acceptance of Information Technology: Toward a Unified View,” *MIS Quarterly*, vol. 27, no. 3, pp. 425–478, 2003.
[38] E. M. Rogers, *Diffusion of Innovations*. The Free Press, 1983.
[39] W. R. Scott, “The Adolescence of Institutional Theory,” *Administrative Science Quarterly*, vol. 32, no. 4, pp. 493–511, 1987.
[40] V. Venkatesh and F. D. Davis, “A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies,” *Management Science*, vol. 46, no. 2, pp. 186–204, Feb. 2000.
[41] D. Skoumpopoulou, A. K. L. Wong, P. M. L. Ng, and M. F. Lo, “Factors that affect the acceptance of new technologies in the workplace: a cross case analysis between UK and Hong Kong,” presented at the UKAIS 2018, Oxford, UK, 2018.
[42] G. Garrison, C. M. R. Jr, and S. H. Kim, “An Identification of Factors Motivating Individuals’ Use of Cloud-Based Services,” *Journal of Computer Information Systems*, vol. 58, no. 1, pp. 19–29, Jan. 2018.
[43] K. ZHU, K. L. KRAEMER, and J. DEDRICK, “Information Technology Payoff in E-Business Environments: An International Perspective on Value Creation of E-Business in the Financial Services Industry,” *Journal of Management Information Systems*, vol. 21, no. 1, pp. 17–54, Jan. 2004.
[44] J. C. Brancheau and J. C. Wetherbe, “The Adoption of Spreadsheet Software: Testing Innovation Diffusion Theory in the Context of End-User Computing,” *Information Systems Research*, vol. 1, no. 2, pp. 115–143, Jun. 1990.
[45] R. B. Cooper and R. W. Zmud, “Information Technology Implementation Research: A Technological Diffusion Approach,” *Management Science*, vol. 36, no. 2, pp. 123–139, Feb. 1990.
[46] M. Ghobakhloo, D. Arias- Aranda, and J. Benitez- Amado, “Adoption of e- commerce applications in SMEs,” *Industrial Management & Data Systems*, vol. 111, no. 8, pp. 1238–1269, Aug. 2011.
[47] M. A. Hameed, S. Counsell, and S. Swift, “A conceptual model for the process of IT innovation adoption in organizations,” *Journal of Engineering and Technology Management*, vol. 29, no. 3, pp. 358–390, Jul. 2012.
[48] H. Gangwar, H. Date, and R. Ramaswamy, “Understanding determinants of cloud computing adoption using an integrated TAM-TOE model,” *Journal of Enterprise Information Management*, vol. 28, no. 1, pp. 107–130, Feb. 2015.
[49] Y. Alshamaila, S. Papagiannidis, and F. Li, “Cloud computing adoption by SMEs in the north east of England: A multi- perspective framework,” *Journal of Enterprise Information Management*, vol. 26, no. 3, pp. 250–275, Apr. 2013.
[50] J.-W. Lian, D. C. Yen, and Y.-T. Wang, “An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital,” *International Journal of Information Management*, vol. 34, no. 1, pp. 28–36, Feb. 2014.
[51] H. P. Borgman, B. Bahli, H. Heier, and F. Schewski, “Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework,” in *2013 46th Hawaii International Conference on System Sciences*, 2013, pp. 4425–4435.
[52] P. Gupta, A. Seetharaman, and J. R. Raj, “The usage and adoption of cloud computing by small and medium businesses,” *International Journal of Information Management*, vol. 33, no. 5, pp. 861–874, Oct. 2013.
[53] C. Low, Y. Chen, and M. Wu, “Understanding the determinants of cloud computing adoption,” *Industrial Management & Data Systems*, vol. 111, no. 7, pp. 1006–1023, Aug. 2011.

[54] O. M. Yigitbasioglu, “The role of institutional pressures and top management support in the intention to adopt cloud computing solutions,” *Journal of Enterprise Information Management*, vol. 28, no. 4, pp. 579–594, Jul. 2015.
[55] A. Abdollahzadegan, A. R. Che Hussin, M. Moshfegh Gohary, and M. Amini, “The Organizational Critical Success Factors for Adopting Cloud Computing in SMEs,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2333028, Aug. 2013.
[56] J. Mingers and J. Brocklesby, “Multimethodology: towards a framework for mixing methodologies,” *Omega*, vol. 25, no. 5, pp. 489–509, 1997.
[57] W. J. Orlikowski and J. J. Baroudi, “Studying information technology in organizations: Research approaches and assumptions,” *Information systems research*, vol. 2, no. 1, pp. 1–28, 1991.
[58] R. Galliers, *Information systems research: Issues, methods and practical guidelines*. Blackwell Scientific, 1992.
[59] D. F. Norris and B. A. Lloyd, “The scholarly literature on e-government: Characterizing a nascent field,” *International Journal of Electronic Government Research (IJEGR)*, vol. 2, no. 4, pp. 40–56, 2006.
[60] M. D. Myers and D. Avison, “An introduction to qualitative research in information systems,” 2002.
[61] R. Galliers, D. Klass, M. Levy, and E. Pattison, “Effective strategy formulation using decision conferencing and soft systems methodology,” presented at the Proceedings of IFIP 8.2 Working Conference on Collaborative Work, Social Communications, and Information Systems (COSCIS), 1991, pp. 157–179.
[62] G. Walsham, “Interpretive case studies in IS research: nature and method,” *European Journal of information systems*, vol. 4, no. 2, pp. 74–81, 1995.
[63] B. J. Oates, *Researching information systems and computing*. Sage, 2005.
[64] C. Cassell and G. Symon, “Qualitative research in work contexts,” *Qualitative methods in organizational research*, pp. 1–13, 1994.
[65] O. K. Ngwenyama and A. S. Lee, “Communication richness in electronic mail: Critical social theory and the contextuality of meaning,” *MIS quarterly*, pp. 145–167, 1997.
[66] H. Kokko and I. Ots, “When not to avoid inbreeding,” *Evolution*, vol. 60, no. 3, pp. 467–475, 2006.
[67] A. Pinsonneault and K. Kraemer, “Survey research methodology in management information systems: an assessment,” *Journal of management information systems*, vol. 10, no. 2, pp. 75–105, 1993.
[68] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A design science research methodology for information systems research,” *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.
[69] M. Bichler, “Design science in information systems research,” *Wirtschaftsinformatik*, vol. 48, no. 2, pp. 133–135, 2006.
[70] A. Guitouni and J.-M. Martel, “Tentative guidelines to help choosing an appropriate MCDA method,” *European Journal of Operational Research*, vol. 109, no. 2, pp. 501–521, 1998.
[71] A. Lin and N.-C. Chen, “Cloud computing as an innovation: Percepetion, attitude, and adoption,” *International Journal of Information Management*, vol. 32, no. 6, pp. 533–540, 2012.
[72] W. Hommel, “Information Security Management and Security Reporting,” in *Encyclopedia of Information Science and Technology, Third Edition*, IGI Global, 2015, pp. 4335–4346.
[73] W. Stallings, “Standards for Information Security Management,” *Internet Protocol Journal*, vol. 10, no. 4, p. 10, 2007.
[74] J. Patil, “Information security framework: case study of a manufacturing organization,” *Mercy College, New York*, 2008.
[75] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.
[76] S. Sethi and S. Sruti, “Cloud Security Issues and Challenges,” in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2018, pp. 77–92.
[77] K. Kark, P. Stamp, J. Penn, L. Koetzle, and J. Mulligan, “Defining A High-Level Security Framework. Putting Basic Security Principles To Work,” 2007.
[78] S. N. Watuthu, “A Framework to Extend COBIT Security Framework to Overcome Confidentiality Threats in Electronic Commerce,” 2015.
[79] United States Public Law, “E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act (FISMA).” Dec-2002.
[80] United States Code, “Federal Information Security Modernization Act of 2014, Public Law 113-283.” 2014.
[81] H. N. Foerstel, *Freedom of information and the right to know: The origins and applications of the Freedom of Information Act*. Greenwood Press Westport, CT, 1999.
[82] P. Law, “Law 104-106: Clinger-Cohen Act of 1996,” 1996.
[83] P. Law, “104-13,” *Paperwork Reduction Act of 1995*, vol. 22, 1995.
[84] P. Act, “The Privacy Act of 1974,” *USA Privacy Act (updated version), last access date*, vol. 16, p. 2011, 1974.
[85] OMB Memorandum M-05-24, “Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.” Aug-2004.
[86] OMB Memorandum M-06-16, “Protection of Sensitive Agency Information.” Executive Office of the President, Jun-2006.

[87] OMB Memorandum M-07-11, “Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.” Mar-2007.
[88] OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC).” Nov-2007.
[89] OMB Memorandum M-08-16, “Guidance for Trusted Internet Connections Statement of Capability (SOC) Form.” Apr-2008.
[90] OMB Memorandum M-08-27, “Guidance for Trusted Internet Connection (TIC) Compliance.” Sep-2008.
[91] OMB Memorandum M-09-32, “Update on the Trusted Internet Connections Initiative.” Sep-2009.
[92] P. FIPS, “140-2,” *Security Requirements for Cryptographic Modules*, vol. 25, 2001.
[93] P. FIPS, “199,” *Standards for Security Categorization of Federal Information and Information Systems*, vol. 2, 2004.
[94] P. FIPS, “200,” *Minimum Security Requirements for Federal Information and Information Systems*, vol. 2, 2006.
[95] P. FIPS, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” *Computer Security Division, National Institute of Standards and Technology*, 2006.
[96] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V.3.0,” 2017.
[97] OMB Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Information Resources.” Nov-2000.
[98] AICPA, “Illustrative Type 2 SOC 2 SM Report with the Criteria in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM),” Apr. 2014.
[99] ISO/IEC, “Code of practice for information security controls based on ISO/IEC 27002 for cloud services”, ISO/IEC 27017:2015 Information technology -- Security techniques,” 2015.
[100] ISO/IEC, “ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,” 2014.
[101] Office of the Privacy Commissioner of Canada, “Personal Information Protection and Electronic Documents Act (PIPEDA,” 2018.
[102] G. D. P. Regulation, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46,” *Official Journal of the European Union (OJ)*, vol. 59, no. 1–88, p. 294, 2016.
[103] Maxico, “Federal Law on Protection of Personal Data Held by Private Parties,” May 2010.
[104] G. Stoneburner, A. Y. Goguen, and A. Feringa, “Sp 800-30. risk management guide for information technology systems,” 2002.
[105] R. Ross, S. Katzke, A. Johnson, M. Swanson, M. Stoneburner, and G. Rogers, “NIST Special Publication 800-37,” *Guide for the Security Certification and Accreditation of Federal Information Systems*, 2004.
[106] P. Mell, T. Bergeron, and D. Henning, “NIST Special Publication 800-40: Creating a patch and vulnerability management program,” *Recommendations of the National Institute of Standards and Technology*, 2005.
[107] T. Grance, J. Hash, S. Peck, J. Smith, and K. Korow-Diks, “SP 800-47. Security Guide for Interconnecting Information Technology Systems,” 2002.
[108] Joint Task Force Transformation Initiative, “SP 800-53 Rev. 3. Recommended Security Controls for Federal Information Systems and Organizations,” 2009.
[109] W. Barker, “NIST Special Publication 800-60 Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories. National Institute of Standards and Technology,” *Computer Security Division*, 2003.
[110] R. Kissel, K. Stine, M. Scholl, H. Rossman, J. Fahlsing, and J. Gulick, “Nist special publication 800-64 revision 2 security considerations in the system development life cycle,” *Nist Special Publication*, pp. 1–34, 2008.
[111] M. Souppaya, “NIST SP 800-70, Revision 2,” *Security Configuration Checklists Program for IT Products–Guidance for Checklists Users and Developers*, 2011.
[112] OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies.” Dec-2003.
[113] OMB Memorandum M-05-24, “Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.” Aug-2004.
[114] OMB Memorandum M-08-22, “Guidance on the Federal Desktop Core Configuration (FDCC).” Nov-2007.
[115] OMB Memorandum M-14-04, “Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management.” Nov-2013.
[116] “Memoranda 02-01 (Guidance for Preparing and Submitting Security Plans of Action and Milestones) (Text Only).” [Online]. Available: https://georgewbush-whitehouse.archives.gov/omb/memoranda/text/m02-01.html. [Accessed: 01-Dec-2018].
[117] OMB Memorandum M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.” Jul-2006.
[118] OMB Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information.” May-2007.

[119] OMB Memorandum M-10-28, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS).” Jul-2010.
[120] M. T. McCarthy, “USA patriot act,” 2002.
[121] B. Obama, “Executive Order 13526: Classified National Security Information,” presented at the United States. Office of the Federal Register, 2009.
[122] Executive Order 10450, “Security requirements for Government employment,” *Federal Register*, vol. 18, no. 82, p. 2489, 1952.
[123] B. E. Fein, “Access to classified information: Constitutional and statutory dimensions,” *Wm. & Mary L. Rev.*, vol. 26, p. 805, 1984.
[124] M-06-06, “Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12.” Feb-2006.
[125] OMB Memorandum M-06-18, “Acquisition of Products and Services for Implementation of HSPD-12.” Jun-2006.
[126] OMB Memorandum M-07-06, “Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials.” Jan-2007.
[127] OMB Memorandum M-08-01, “HSPD-12 Implementation Status.” Oct-2007.
[128] OMB Circular A-11, “Preparation, Submission and Execution of the Budget.” Jun-2006.
[129] OMB Memorandum M-03-22, “Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.” Sep-2003.
[130] OMB Circular A-123, “Management’s Responsibility for Internal Control.” Dec-2004.
[131] OMB Memorandum M-15-14, “Management and Oversight of Federal Information Technology.” Jun-2015.
[132] OMB Memorandum M-00-13, “Privacy Policies and Data Collection on Federal Web Sites.” Jun-2000.
[133] OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure.” Aug-2008.
[134] OMB Memorandum M-00-07, “Incorporating and Funding Security in Information Systems Investments.” Feb-2000.
[135] T. K. Damenu and C. Balakrishna, “Cloud Security Risk Management: A Critical Review,” presented at the Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on, 2015, pp. 370–375.
[136] X. Yang, “Framework development in plant disease risk assessment and its application,” in *Plant disease epidemiology: facing challenges of the 21st Century*, Springer, 2006, pp. 25–34.
[137] K. Sadgrove, *The complete guide to business risk management*. Routledge, 2016.
[138] A. Lehar, “Measuring systemic risk: A risk management approach,” *Journal of Banking & Finance*, vol. 29, no. 10, pp. 2577–2603, 2005.
[139] C. J. Alberts and A. Dorofee, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc., 2002.
[140] R. K. Otto and K. S. Douglas, *Handbook of violence risk assessment*. Routledge, 2011.
[141] C. D. Carrington and P. M. Bolger, “Uncertainty and risk assessment,” *Human and Ecological Risk Assessment: An International Journal*, vol. 4, no. 2, pp. 253–257, 1998.
[142] E. J. Riedl and G. Serafeim, “Information risk and fair values: An examination of equity betas,” *Journal of accounting research*, vol. 49, no. 4, pp. 1083–1122, 2011.
[143] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing octave allegro: Improving the information security risk assessment process,” CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2007.
[144] S. Gregor and A. R. Hevner, “Positioning and presenting design science research for maximum impact.,” *MIS quarterly*, vol. 37, no. 2, 2013.
[145] S. Klipper, “ISO 27005 und BSI IT-Grundschutz,” in *Information Security Risk Management*, Springer, 2015, pp. 97–106.
[146] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, “Current challenges in information security risk management,” *Information Management & Computer Security*, vol. 22, no. 5, pp. 410–430, 2014.
[147] A. Rot and B. Olszewski, “Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection,” presented at the In 2017 Federated Conference on Computer Science and Information Systems, 2017, vol. 13, pp. 113–117.
[148] M. W. Harkins, “Emerging Threats and Vulnerabilities: Reality and Rhetoric,” in *Managing Risk and Information Security*, Springer, 2016, pp. 81–98.
[149] K. Tidwell, K. Saurabh, D. Dash, H. S. Njemanze, and P. S. Kothari, “Threat detection in a network security system,” Aug. 2007.
[150] B. Karabacak and I. Sogukpinar, “ISRAM: information security risk analysis method,” *Computers & Security*, vol. 24, no. 2, pp. 147–159, 2005.
[151] J. Lopez and Institute for Systems and Technologies of Information, Control and Communication, Eds., *A security metrics framework for the Cloud*. Piscataway, NJ: IEEE, 2011.
[152] K. J. Hole and L.-H. Netland, “Toward Risk Assessment of Large-Impact and Rare Events,” *IEEE Security & Privacy Magazine*, vol. 8, no. 3, pp. 21–27, May 2010.
[153] P. Shamala, R. Ahmad, and M. Yusoff, “A conceptual framework of info structure for information security risk assessment (ISRA),” *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45–52, Jul. 2013.

[154] M. S. Lund, B. Solhaug, and K. Stølen, “Risk Analysis of Changing and Evolving Systems Using CORAS,” in *Foundations of Security Analysis and Design VI*, vol. 6858, A. Aldini and R. Gorrieri, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 231–274.
[155] S. R. Patil and H. C. Frey, “Comparison of Sensitivity Analysis Methods Based on Applications to a Food Safety Risk Assessment Model,” *Risk Analysis*, vol. 24, no. 3, pp. 573–585, Jun. 2004.
[156] S. T. Mortimer and D. Mortimer, *Quality and Risk Management in the IVF Laboratory*, 2nd ed. Cambridge: Cambridge University Press, 2015.
[157] H. Wang, J. Mylopoulos, and S. Liao, “Intelligent agents and financial risk monitoring systems,” *Communications of the ACM*, vol. 45, no. 3, pp. 83–88, Mar. 2002.
[158] R. Saint-Germain, “Information security management best practice based on ISO/IEC 17799,” *INFORMATION MANAGEMENT JOURNAL-PRAIRIE VILLAGE-*, vol. 39, no. 4, p. 60, 2005.
[159] H. Van der Haar and R. Von Solms, “A model for deriving information security control attribute profiles,” *Computers & Security*, vol. 22, no. 3, pp. 233–244, 2003.
[160] C. C. Wood, “An unappreciated reason why information security policies fail,” *Computer Fraud & Security*, vol. 2000, no. 10, pp. 13–14, 2000.
[161] G. V. Post and A. Kagan, “Evaluating information security tradeoffs: Restricting access can interfere with user tasks,” *Computers & Security*, vol. 26, no. 3, pp. 229–237, 2007.
[162] K. D. Loch, S. Conger, and E. Oz, “Ownership, privacy and monitoring in the workplace: a debate on technology and ethics,” *Journal of Business Ethics*, vol. 17, no. 6, pp. 653–663, 1998.
[163] R. Baskerville and M. Siponen, “An information security meta-policy for emergent organizations,” *Logistics Information Management*, vol. 15, no. 5/6, pp. 337–346, 2002.
[164] M. E. Whitman, A. M. Townsend, and R. J. Aalberts, “Information systems security and the need for policy,” in *Information security management: Global challenges in the new millennium*, IGI Global, 2001, pp. 9–18.
[165] R. E. Bellman and L. A. Zadeh, “Decision-making in a fuzzy environment,” *Management science*, vol. 17, no. 4, p. B-141, 1970.
[166] F. S. Jalayer and A. Nabiollahi, “Ranking Criteria of Enterprise Information Security Architecture using Fuzzy TOPSIS,” *International Journal of Computer Science & Information Technology*, vol. 8, no. 5, 2016.
[167] C. SJ, C. Hwong, S. Chen, and C. Hwong, “Fuzzy multiple attribute decision-making: methods and applications,” *книга*, 1992.
[168] M. Pandey, N. Khare, and S. Shrivastava, “New Aggregation Operator for Trapezoidal Fuzzy Numbers based on the Geometric Means of the Left and Right Apex Angles,” *Submitted for Publication*, 2012.
[169] C. E. Shannon, “A mathematical theory of communication,” *ACM SIGMOBILE mobile computing and communications review*, vol. 5, no. 1, pp. 3–55, 2001.