CHAPTER 05: CONCLUSION

5.1 Introduction

The objective of this chapter is to provide summary of the results discovered through the research study. Different categories of figures, analysis data and information are based to the study. Further recommendations, limitations and areas of further studies are also being taken in to discussion at the final part of the thesis.

5.2 Conclusion

The study identified several important factors impact to business continuity of local telecommunication companies based on information security measures outlined in ISO27001. Convincing customers and investors of information security, building confidence in order to protect information are some of the success factors strengthening the confidentiality, integrity and availability of information.

At present organization structure and security policies have been recognized as one of the significant factors in the business continuity by country's telecommunication operators. Over 52% responded positively to this. Further higher management (75.36%) and middle management (52.68%) of telecommunication companies acknowledged this as business continuity factor. Especially higher management commitment, assigning roles and responsibilities, incident management, security policies etc. are major components for identifying organizational structure and security policies as a business continuity factors. Further these factors laid strong foundation and successful implementation of them set a path to succeed other factors in business continuity strategy. Aligning these with the other factors is a definite advantage for the success of entire business strategy in the organization. For an example higher management commitment such as identifying key functional areas, assigning responsibilities, formulation of business strategies etc. affect most of areas in information systems functionality in the telecommunication domain. True significance has been identified by the fixed line operators (53.2%) and mobile (64.47%) operators respectively.

Management of information assets is an extremely important factor in both information and business security aspects. Information assets are considered to be core of the business functionality in modern corporate business. Particularly in telecommunication domain it has direct impact to business operations. In general 52.3% of them have acknowledged that this has influence to business operations. Despite the economic pressure especially in telecom sector, companies continue to invest in information assets and information security in larger scale and this demonstrates the legitimacy of this factor. 74.24% of the higher management in telecommunication companies and 89.40% of fixed line operators, 55.55% of mobile operators undoubtedly indicated the magnitude of asset management practices as a sustainability aspect to their operations. On the other hand, almost all the telecom operators recognized the actual strategic value of this factor.

During the study, it has been identified that physical and environmental security are factors that give a high contribution to telecommunication sector in terms of security and business continuity. Respectively 72.22%, 75.16% of higher and middle managements stated the importance of such factors. Principally protection of information systems against natural and manmade disasters are considered in greater detail, since all the functional resources rely on the safety of information resources. As a fact, 44.21% of fixed line operators, 70.12% of mobile operators emphasize the importance of minimizing the impact of natural and manmade threats throughout the assessment. General observation discloses that 71% of them are concerned in adopting such controls not only securing their information assets but also to assure the sustainability of information systems functionality.

Information systems functionality is helpful for effective operations. Hence an important question is being answered. “Can information systems effectively function without proper operational and procedural approaches?" As a result of the involvement of different layers of the organization to the functional operations of the information systems, to facilitate expected services, technological and procedural level approaches are mandatory to implement. Thus 52% of the occupants in local telecommunication sector designate that communication and operational practices as one of the principal factors in business continuity process. Further this has directly impact the daily functionality of systems related divisions in the business. Failing to identifying the practices result in malfunction of daily operations. Exclusively 62% of the middle management of telecom operators recognized the importance of such measures, since most of the decisions with respect to short term operations are initiated at this level. Therefore communication and operational management practices have been identified as another important information security measure that affect business continuity of telecommunication operations.

Existence of a regulatory organization and standards are vital factors for long term development of the industry. Involvement of regulatory authorities ensures proper governance of the industry, whereas standards secure establishment of structured system practices in the organization. One of the significances of the study was, 96% of telecom operators articulated that present business continuity practices introduced by Telecommunication Regulatory Commission of Sri Lanka is not adequate to cater the country's telecommunication requirements pertaining to information security and business continuity. However high responses were recorded in acceptance of standards such as ISO 27001, to improve business continuity and information security. The early adopters can potentially gain competitive advantages, hence globally incorporating of information security standards have increased up to 15% and will continue to increase. This has been identified undoubtedly by higher administration (78.25%) of local telecommunication companies. However in summarizing the above information illustrated , implementation of organizational structure and security policy, adaptation of assets management practices, implementation of physical and environmental security technologies, adaptation of communication and operational practices have positive impact on business continuity of Sri Lankan telecommunication operators.

5.3 Recommendation

Recommendation to the Telecommunication Regulatory Commission of Sri Lanka

Existence of governance authority is vital factor for long term development of any industry. Telecommunication Regulatory Commission of Sri Lanka chartered as the main governance authority for telecommunication related operations in the country. Growth of countries fixed line telephone density from 121388 to 3599250 in between 1990-2011 and mobile cellular from 2644 in 1992 to 18,176,030 in 2011 (TRCSL Statistical overview ,2011) emphasized the presence of well establish framework empowered by different laws , regulations and practices. It is interesting to note that TRCSL had not much departed from its main objectives and other responsibilities with the rapid development of the industry. On the other hand, timely changes to governance structure including laws, regulations, standards and practices have not completely taken in to consideration. As a result of the study, it was identified that present business continuity practices enforced by TRCSL is not sufficient. Especially 96% of the participants to the research survey highlighted the same fact. Further compare to the other regional and global telecommunication regulatory authorities, commitment of TRCSL in such practices are far behind. Being one of the rapidly growing industries, non-existence of such vital regulatory provisions and practices are serious issue to be resolved. Hence TRCSL must engage in introducing such resolutions to country’s telecommunication governance structure. However following strategies can be proposed to incorporate in to the process.

- Introducing such amendments to country’s telecommunication sector is time consuming effort. Hence short term and long term strategy based approach would applicable to full fill such requirements. Success of short term strategies can be incorporate to formulate long term strategies.

- Introduce industry best practices adopt by the other regional and global authorities pertaining to business continuity to Sri Lankan telecommunication sector.
- Encourage local telecommunication operators to adopt internationally accepted standards to maintain business continuity.
- Formulation of new laws, regulations and statutory amendments to existing governance structure.

Information security and business continuity are few of the driving forces in modern telecommunication era. Hence to enrich local governance framework, directives can be obtain through regionally and globally recognized statutory bodies, organizations, committees etc. However due to the complex nature of telecommunication operations, different systems are interconnected irrespective of national and geographical boundaries. Hence confidentiality, integrity and availability of information become one of the prime responsibilities of telecom operators. Therefore introducing of information security and business continuity standards, legislative provisions, practices etc. are required than ever before in local context.

Recommendation to the Telecommunication Operators

It has been identified that demand and interest to the standards for information security increased by 70% and adoption of security standards increased by 9% globally. (Ernst & Young’s, 2008). The whole impression behind such interest is to secure organization information assets and to provide uninterruptable service to maintain business operations. Hence it was recommended to adopt internationally accepted standards and other practices pertaining to business continuity to face the local and global competition and assure sustainability of the business operations. On the other hand adoption of such practices indirectly overstretched TRCSL to introduce comprehensive information security practices pertaining to business continuity to country’s telecommunication governance structure. One of the significances highlighted during the study was the low awareness reflected from professional and engineering category to the surveyed entities. Higher management and middle management of the local telecommunication companies have responded fairly to the survey. On the other hand managerial strategies initiated from higher levels are being place into functional status by the employees occupied at this level. Moreover these employees are highly subject oriented employees. Limitation of time availability to focus on such concepts and practices is another reason. On the other hand good knowledge of these concepts are definite advantage for professional and engineering category employees to improve business competencies .Hence to overcome such instances, local telecommunication companies require greater concern to allocate more resources such as financial provisions, training opportunities etc. during the initiation of their annual business strategy to facilitate latest knowledge and develop skills to such employees.

5.4 Limitations

Objective of this study is to investigate the impact of information security measures outline in ISO27001 to the business continuity in Sri Lankan telecommunication companies. However several limitations were identified with regard to research study. Any further research carried-out using this as a base should consider limitations along with the result.

This study was conducted within a limited time period. Initial scope was comparatively large due to the characteristics of the subject domain .Hence study was further narrowed by the researcher and restricted to limited factors. Selected sample wasn't purely representing characteristics required by the researcher, but it was only trusted source available at the time of the study.

Local resources such as research papers, publications and statistics related to the study are very limited. Hence Internet was the main information resource provider to the study. On the other hand most facts such as statistical figures, research papers etc. are financially valued by the respective authors and procuring them was another challenge to the researcher.

Due to the sensitivity of the study, there wasn't any mechanism to verify the validity of the answers provided by the employees of local telecommunication companies.

5.5 Further Directions

This study can be incorporated in to future studies in the field of information security. However following list provide some relative areas future researches can focus on.

- This study was conducted to investigate effect to the business continuity of local telecommunication companies based on ISO 27001 security measures. Generalized results were aimed at this study. Therefore future studies can be focus in to investigate individual security measures and their impact to the business continuity of local telecommunication domain.

- All the local telecommunication operators were focused to the study. Hence future researchers can extend their studies in to different categories of telecom operators such as mobile, fixed etc. in the country. This will enable them to further narrow down the study in to more specific segments. This will help them to capture more specific reasons caused to business continuity.

- Future researchers can extend their studies to investigate impact to the business continuity from all the defined information security measures outline in ISO 27001.

- Information extract from this study can be utilized for further studies to discover information security factors and their impact to the business continuity in broader and comprehensive manner

REFERENCES

Alan Gillis, 2008, *‘Improving the quality of information security management systems with ISO27000’*, Emerald Journal.

AT&T, 2006, *‘Key Elements to an Effective Business Continuity Plan - Information Security Management Objectives and Practices’*.

AT&T, 2011, ‘*Business Continuity Preparedness Handbook’*.

AT&T, 2011,*’Business Continuity Preparedness Handbook: key elements to an affective business continuity plan’*.

British Broadcasting Corporation, 2009,’*Business Continuity Management Policy’*, (V4).doc.

BS ISO/IEC 27001:2005 BS7799-2:2005, *Information Security Technology- Security Techniques -Information Management Systems –Requirement.*

Central Bank of Sri Lanka, 2009, Annual Report.

David Pollitt, 2005, ‘*Energies Trains Employees and Customers in IT Security’*, Emerald Journal, VOL. 13, NO. 2, pp. 25-28.

Eduardo Gelbstein, Ahmad Kamal, 2002,*'Information Insecurity'* United Nations ICT Task Force & Institute of Training and Research.

Edward S. Talley, John J. Reeves, 2003,*'Federal Legislative and Regulatory Business Continuity Requirements for the IRS',* Center for Enterprise Modernization', McLean Virginia, Version 1.0.

Elizabeth Lomas, 2008,*'Information governance: information security and access within a UK context'*,Northumbria University.

Elizabeth Lomas, 2010,*'Information governance:information security and access within a UK context'*,Northumbria University.

Ernst & Young, 2010,*'Business Continuity Planning in the Telecommunication Industry'*.

Ernst & Young, 2010, *'Business Continuity Planning in the Telecommunication Industry'*.

Ernst & Young, 2011,*'Insight on IT Risk: Information Security in a Borderless World'*.

Ernst & Young's, 2008,*'Manage beyond Compliance',Global Information Security Survey*.

Ernst & Young's, 2010,*'Borderless Security: Global Information Security Survey'*.

European Union, 2001,*'Network and Information Security',*Proposal for a European Policy Approach.

Gauri Moragoda, 2006,*'Brief Overview of Telecommunication Law in Sri Lanka'*,
National Information Technology Conference.

Harold F.Tipton and Micki Krause, 2002,*'Information Security Management Handbook'*, Boca Raton: CRC Press LLC.

Herbert Bertine, Igor Faynberg,Hui-Lan Lu,2004,*'Overview of Data and Telecommunications Security Standardization Efforts in ISO, IEC,ITU, and IETF'*,Bell Labs Technical Journal.

International Telecommunication Union, 2000-2010, ICT indicator Database.

International Telecommunication Union, 2010, *'The World in 2010'* ICT Facts and Figures.

International Telecommunication Union,2009, *'Security in telecommunications and information technology- An overview of issues and the development of existing ITU-T recommendations for secure telecommunications'*4th Edition.

Jacques Both,Rossouw Von Solms,2004,*'A Cyclic Approach to Business Continuity Planning'*,Information Management & Computer Security ,Vol.12 No.4,pp. 328-337.

Jane Merete Hagen, Eirik Albrechtsen, Jan Hoyden, 2008,*'Implementation and effectiveness of organizational information security measures'*, Norwegian University of Science and Technology.

Janne Merete Hagen Eirik Albrechtsen ,Hovden , Eirik Albrechtsen , Jan Hovden ,*' Implementation and Effectiveness of Organizational Information Security Measures'.*

John W. Rittinghouse, Ph.D., CISM/James F. Ransome, Ph.D., CISM, CISSP,' *Business Continuity and Disaster Recovery for InfoSec Managers'.*

Jun Sun,Punit Ahluwalia,Kai S.Koong,2011,*'The more secure the better-A study of information security readiness'*,The University of Texas.

K.C.Usgodaarachchi , 2006 Dec , *'Maturity of Business Continuity Management and ICT Reliance is Sri Lanka'* , MBA IT University of Moratuwa.

KPMG, 2008,'2008 Continuity Insights and KPMG Advisory Services: '*Business Continuity Management Benchmark Report'.*

KPMG, 2011 *'Information Security in Telecom Sector'.*

Michigan Technological University, 2011,*'Information Security Plan'.*

National Institute of Standards and Technology, U.S.Department of Commerce, 2010,*'Information Security: Guide for Appling the Risk Management Framework to Federal Information Systems'.*

Pricewaterhousecoopers, 2011,' *Global State of Information Security Survey'.*

Qingxiong Ma, Warrensburg, Allen C.Johnston, J. Michael Pearson, 2008,*'Information security management objectives and practices: a parsimonious framework'.*

Sri Lanka Telecommunications, 1991, ACT, No.25 Of 1991.

Sri Lanka Telecommunications, 1996, ACT (Amendment), No.27 of 1996.

Sumathi Dharmawardena, 2006,*'Telecommunication Regulations in Sri Lanka'*, National Information Technology Conference.

Telecommunication Regulatory Commission of Sri Lanka, 2011,*' Statistical Overview 2011'*.

US Department of Commerce, 2010,*'Guide for Applying the Risk Management Framework to Federal Information Systems'*,A Security Life Cycle Approach.

VeriSign, 2005, *'Effective Strategies for Risk Management Business-Process Protection through Assessment, Planning, and Recovery'*.

Virginia Cerullo and Michael J.Cerullo, 2004,*'Business Continuity Planning: A Comprehensive Approach'*.

Wade H.Baker,Alex Hutton,C.David Hylender,Christopher Novak,Christopher Porter,Bryan Sartin,Peter Tippett,J. Andrew Valentine,2009,*'Data Breach Investigation Report*',Verizon Business RISK Team.

World Bank, 2010,*'Year Review'*, Annual Report

APPENDIX I - Questionnaires

Demographic details

1. What best describes your organization business type

   ( ) Fixed line operator

   ( ) Mobile operator

   ( ) Fixed Line and Mobile Operator

2. What services are available to the market

   ( ) Voice services, Data services, Video services

   ( ) Voice services and Data services

   ( ) Voice services only

   ( ) Data services only

3. What scale best describes the size of your organization

   ( ) 01-100

   ( ) 100-500

   ( ) 500-1000

   ( ) 1000-1500

   ( ) 1500-2000

   ( ) Over 2000

4. Which title most accurately list your position within your organization

   ( ) Consultant

   ( ) Higher management

   ( ) Middle management

   ( ) Professional /Engineering

   ( ) Technical

   ( ) Other: [ ]

5. Gender

   ( ) Male

   ( ) Female

6. Your age group

   ( ) Under 18

   ( ) 18-24

   ( ) 24-36

   ( ) 37-48

   ( ) 49-64

   ( ) Over 64

Management Commitment

7. How do you evaluate importance of the management commitment for successful implementation of business continuity plan

   ( ) Very important

   ( ) Important

   ( ) Neither important nor less important

   ( ) Less important

   ( ) Not important

8. My organization has Senior Management Advisory or Steering committee that provides input and assistance in the preparation, implementation, evaluation and revision of all the business continuity related functional areas in the business

   ( ) Strongly agreed

   ( ) Agreed

   ( ) Neither Agree nor Disagree

   ( ) Disagree

   ( ) Strongly disagree

9. How significant is the documented Business continuity and disaster recovery policy to your organization

   ( ) Very important

   ( ) Important

   ( ) Neither important nor less important

   ( ) Less important

   ( ) Not important

Define Roles and Responsibilities

10. My Organization has a Business continuity planning and disaster recovery committee with clearly defined duties and responsibilities

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

11. BCP Responsibilities and tasks for individuals are approved by the management in my organization

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

12. Disaster Recovery elements such as DR Sites , DR teams , emergency call trees etc. are clearly defined and made available to respective parties in my organization

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

Proper institutionalize incident management practices

13. Formal reporting procedures are exist in the business process to communicate incidents to the management channels

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

14. Your satisfaction about the control measures taken against the reported incidents

( ) Highly satisfied

( ) Satisfied

( ) Neither satisfied nor unsatisfied

( ) Unsatisfied

( ) Highly unsatisfied

Periodic evaluation of Disaster recovery plan

15. How often the management conducts business continuity and disaster recovery security policy reviews, evaluates and communicates same to the relevant parties in the organization

( ) Every 6 months

( ) Every 12 months

( ) Every 18 months

( ) Every 24 months

( ) Never conduct

16. Your satisfaction on effectiveness of testing Disaster Recovery plan within organization

( ) Highly satisfied

( ) Satisfied

( ) Neither satisfied nor unsatisfied

( ) Unsatisfied

( ) Highly unsatisfied

Assets Classification

17. My organization maintains an inventory or registry of the important assets related with the information such as asset custodian, contingency plan for respective asset, external contactable parties etc.

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

18. My understanding of usefulness of asset classification in my organization

    ( ) Very useful

    ( ) Useful

    ( ) Neither useful nor less useful

    ( ) Less useful

    ( ) Not useful

19. Organization conducts risk assessments

    ( ) Every 3 months

    ( ) Every 6 months

    ( ) Annually

    ( ) Randomly

    ( ) Never

Business Impact Analysis

20. “Conducting business impact analysis on critical business functions are important to maintain business continuity in my organization” .How do you evaluate this statement

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

21. My organization identifies and evaluates in advance the probable loss of critical business functions in the event of failure

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

Physical Security Practices

22. Your level of satisfaction of implemented physical entry controls such as barriers, locks, access cards, guards etc in your organization to protect secure areas from unauthorized access is

    ( ) Very high

    ( ) High

    ( ) Neither high nor medium

    ( ) Medium

    ( ) Low

23. My organization has taken adequate precautions to protect equipments from failure of support utilities such as electricity systems, air conditioning systems etc

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

Environmental Security Practices

24. My organization has taken adequate precautions to protect equipment from natural disasters such as flood, earthquakes, fire ,civil unrest, terrorism etc

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

25. My organization has taken adequate precautions to protect equipment from manmade disasters such as civil unrest, terrorism, labor disputes, industrial actions etc.

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

Positioning of appropriate policies and procedures

26. Operating guidelines such as equipment maintenance, backup procedures, systems access, monitoring etc are properly defined, reviewed and made available to all the required parties in my organization

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

27. My organization takes adequate precautions to maintain uninterruptable service with the vendors/suppliers in the event of disasters such as flood, earthquakes, fire, civil unrest, terrarium etc

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

28. Communication procedures /guidelines such as accessing to and configuring firewalls, ACL's, DMZ, monitoring etc. are properly defined, reviewed and made available to all the required parties in my organization

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

Positioning of appropriate technologies

29. User access controls such as password, privileges, rights etc. are important and deployed according to the recommended levels

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

30. Access to the systems such as operating systems, application systems, appliances etc. are controlled and reviewed periodically

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

31. Keeping information and systems backup and regular testing of them are important to maintain integrity and availability of the information

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

32. How important are the implementation of network access controls such as firewalls, IDS, access lists, DMZ etc. in your organization

    ( ) Highly Important

    ( ) Very Important

    ( ) Neither High nor Very important

    ( ) Important

    ( ) Less important

33. Are you satisfied with the recent network access controls such as firewalls, IDS, access lists, DMZ etc. deployed in your environment

    ( ) Highly satisfied, no improvements needed

    ( ) Satisfied, but minor improvements needed

    ( ) Neither satisfied nor unsatisfied

    ( ) Unsatisfied, but can be improved

    ( ) Unsatisfied at all

Enforcement of laws and regulations from legislative authorities

34. How do you define the roll of a regulatory body with regard to the business continuity in telecommunication industry

    ( ) Highly important

    ( ) Very important

    ( ) Neither very important nor important

    ( ) Important

    ( ) Less important

35. How do you evaluate the applicability of existing the regulations and laws to the business continuity in the telecommunication industry

( ) Majority of laws and regulations are applicable

( ) Most of the laws and regulations are applicable

( ) Neither most of the laws and regulations nor few laws and regulations are applicable

( ) Few laws and regulations are applicable

( ) Laws and regulations are not applicable

36. Your overall estimation of impact of laws and regulations to the business continuity in your organization

( ) Very High impact to the business operations

( ) High impact to the business operations

( ) Neither high impact nor Low impact to the business

( ) Low impact to the business operations

( ) No impact at all to the business operations

Adopting standardization

37. Your overall estimation of the impact from standards such as ISO 27001 to the business continuity in your organization

( ) Very High impact to the business operations

( ) High impact to the business operations

( ) Neither high impact nor low impact to the business operations

( ) Low impact to the business operations

( ) No impact at all to the business operations

Business Continuity -Time

38. Time taken to implement information security measures such as environmental security , communication, operational and assets management ,formation of policies ,procedures ,processes etc to improve business continuity in my organization is

    ( ) Significantly low and completed prior to scheduled time period

    ( ) Completed within scheduled time period

    ( ) Neither completed within schedule time nor additional time taken to complete

    ( ) Additional time period taken to complete

    ( ) Never made any attempt to complete

Business Continuity - Improvement

39. Improvements in the operations due to business continuity planning such as information and equipment security , operational and communication policies ,procedures etc. over the recent past in my organization is

    ( ) Significantly high

    ( ) Very high

    ( ) Neither very high nor medium

    ( ) Medium

    ( ) Low

40. “Organization image ,profitability ,credibility have been enhanced over the recent past due to appropriate business continuity planning in my organization” How do you evaluate this statement

( ) Strongly agreed

( ) Agreed

( ) Neither Agree nor Disagree

( ) Disagree

( ) Strongly disagree

APPENDIX II - Pre Survey Questionnaire

1. How do you evaluate the importance on information security to the business

   ( ) Very important

   ( ) Important

   ( ) Neither Important nor Less important

   ( ) Less important

   ( ) Not important

2. “Maintaining business continuity is highly important and prime objective in telecommunication sector “How do you evaluate this statement.

   ( ) Strongly agreed

   ( ) Agreed

   ( ) Neither Agree nor Disagree

   ( ) Disagree

   ( ) Strongly disagree

3. My organization concern standards as important part of their business continuity strategy.

   ( ) Strongly agreed

   ( ) Agreed

   ( ) Neither Agree nor Disagree

   ( ) Disagree

   ( ) Strongly disagree

4. How significant is the following factors to continuation of the business operations.

Factor	**Highly Important**	**Very Important**	**Important**	**Less Important**
Security policy				
Organization of information security				
Assets management				
Human resource security				
Physical and environmental security				
Communication and operational management				
Asses control				
Information systems acquirements of information systems				
Information security incident management				
Business continuity management				
Compliance				

5. "Compliance with legal requirements, security policies and standards are important factors in both security and business continuity aspects" How do you evaluate this statement.

   ( ) Strongly agreed

   ( ) Agreed

   ( ) Neither Agree nor Disagree

   ( ) Disagree

   ( ) Strongly disagree

6. My organization consider information systems acquisition ,development and maintenance features such as data validation, software development , test system protection ,source code security as essential part of business continuity strategy .

   ( ) Strongly agreed

   ( ) Agreed

   ( ) Neither Agree nor Disagree

   ( ) Disagree

   ( ) Strongly disagree

7. Management of information security incidents as essential in company's business strategy.

   ( ) Strongly agreed

   ( ) Agreed

   ( ) Neither Agree nor Disagree

   ( ) Disagree

   ( ) Strongly disagree

8. Management commitment , allocation of responsibilities ,security policy are ;

   ( ) Part of the security strategy

   ( ) Part of the business continuity strategy

   ( ) Neither part of the security strategy nor business continuity strategy

   ( ) Part of both security and business continuity strategy

   ( ) None of the above

9. Information processing facilities are access and managed by external parties in my organization.

   ( ) Strongly agreed

   ( ) Agreed

   ( ) Neither Agree nor Disagree

   ( ) Disagree

   ( ) Strongly disagree

10. Information assets classification and analysis of impact from them to the business is part of my organization's policy

    ( ) Strongly agreed

    ( ) Agreed

    ( ) Neither Agree nor Disagree

    ( ) Disagree

    ( ) Strongly disagree

11. How do you evaluate the contractors and third party employee's engagement in company's business operations?

    ( ) Very important

    ( ) Important

    ( ) Neither Important nor Less Important

    ( ) Less important

    ( ) Not important

12. “Equipment and premises are vital factors in providing security and business functionality to any organization” How do you evaluate this statement.

( ) Strongly agreed

( ) Agreed

( ) Neither Agree nor Disagree

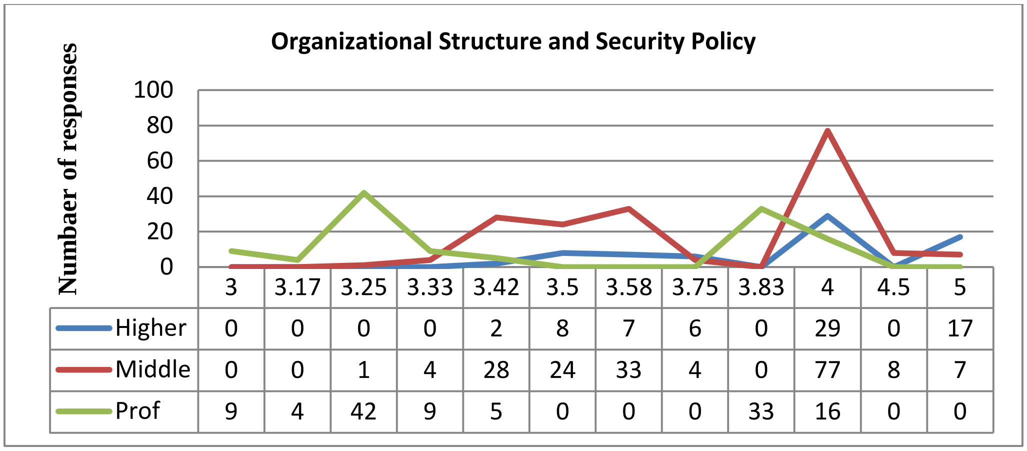
( ) Disagree

( ) Strongly disagree

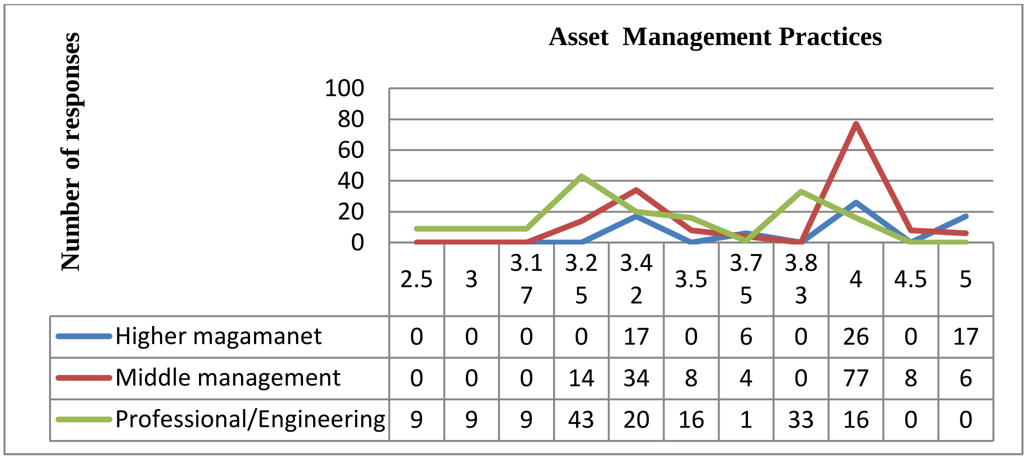
13. Which of the following factors have direct impact on maintain business operations in your organization.

Factor	**Direct Impact**	**Less Impact**
Operational procedures and responsibilities		
Third party service delivery management		
System planning and acceptance		
Protection against malicious and mobile code		
Back-up		
Network Security and management		
Media handling		
Exchange of information		
Electronic commerce services		
Monitoring		
Business requirement for access control		
User access management		
User responsibilities		
Network access control		
Operating system access control		
Application and information access control		
Mobile computing and teleworking		

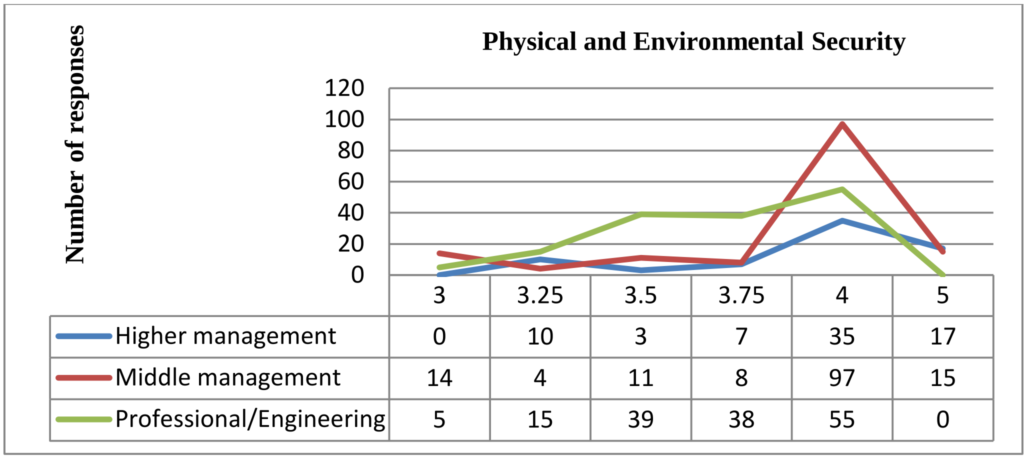
APPENDIX III – Data Analysis - Job Category


Organizational Structure and Security Policy

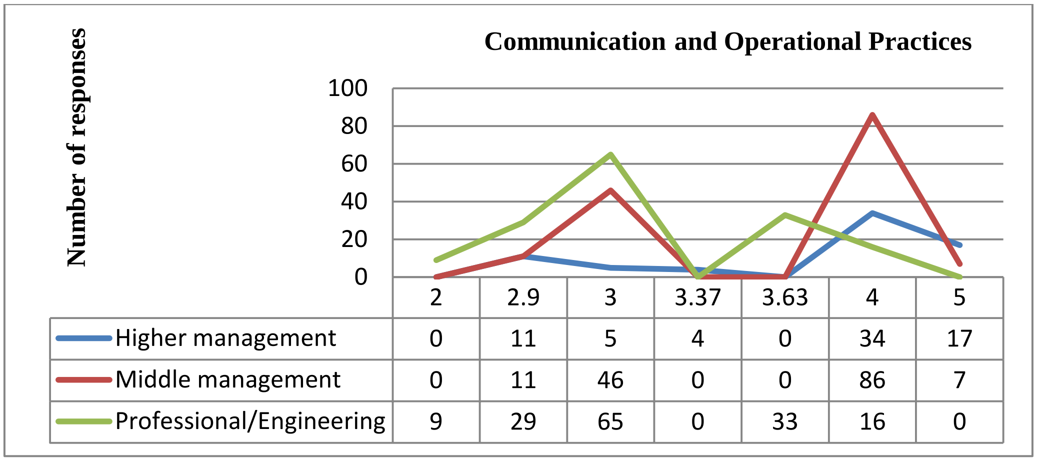
	3	3.17	3.25	3.33	3.42	3.5	3.58	3.75	3.83	4	4.5	5
Higher	0	0	0	0	2	8	7	6	0	29	0	17
Middle	0	0	1	4	28	24	33	4	0	77	8	7
Prof	9	4	42	9	5	0	0	0	33	16	0	0


Asset Management Practices

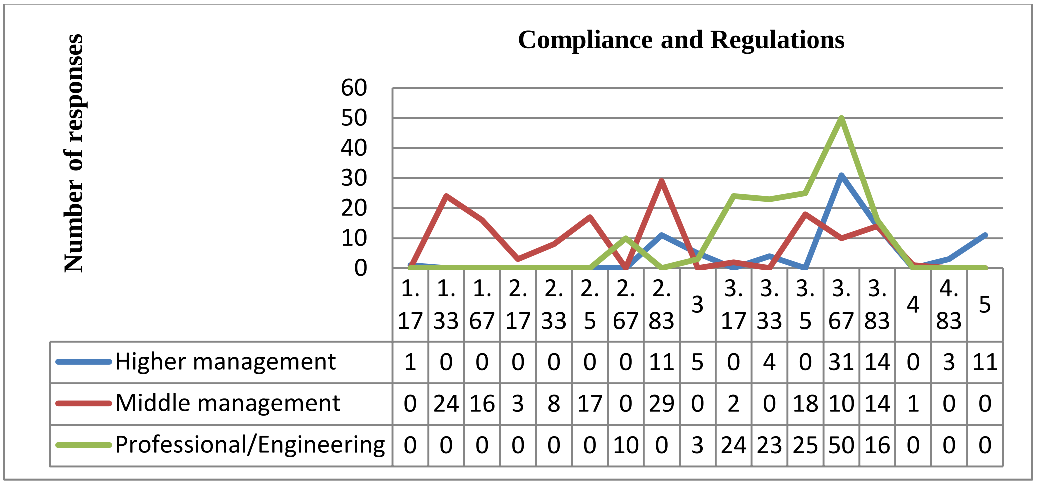
	2.5	3	3.17	3.25	3.42	3.5	3.75	3.83	4	4.5	5
Higher magamanet	0	0	0	0	17	0	6	0	26	0	17
Middle management	0	0	0	14	34	8	4	0	77	8	6
Professional/Engineering	9	9	9	43	20	16	1	33	16	0	0


Physical and Environmental Security

	3	3.25	3.5	3.75	4	5
Higher management	0	10	3	7	35	17
Middle management	14	4	11	8	97	15
Professional/Engineering	5	15	39	38	55	0

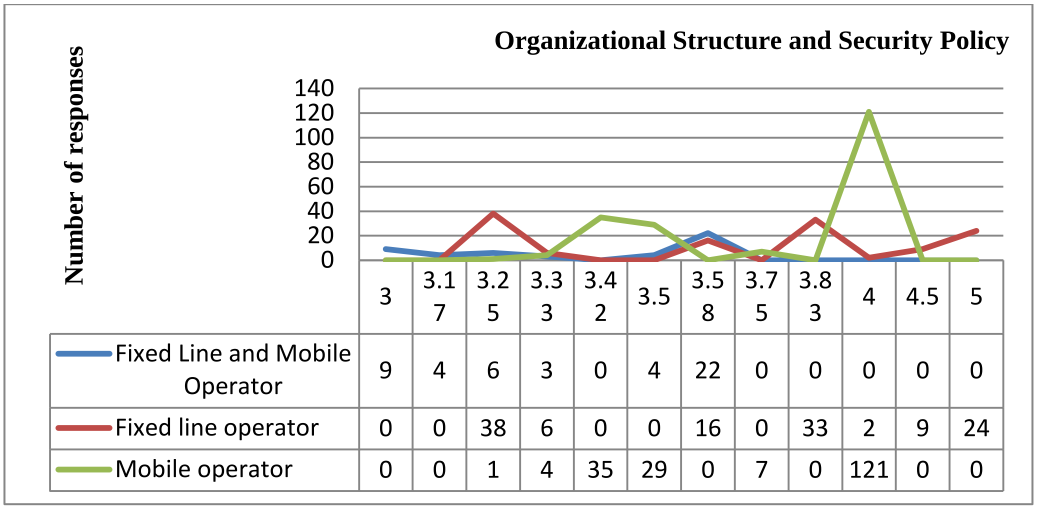


	2	2.9	3	3.37	3.63	4	5
Higher management	0	11	5	4	0	34	17
Middle management	0	11	46	0	0	86	7
Professional/Engineering	9	29	65	0	33	16	0

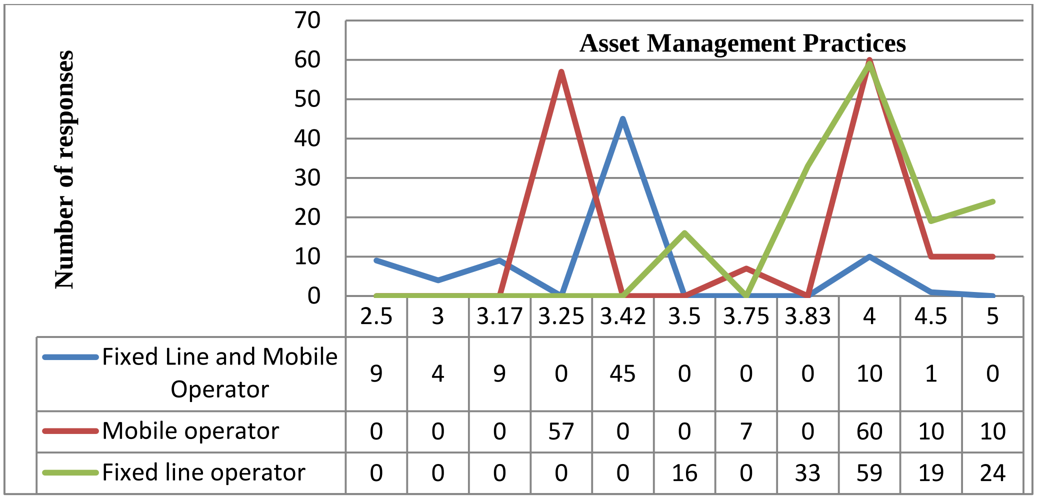


	1.17	1.33	1.67	2.17	2.33	2.5	2.67	2.83	3	3.17	3.33	3.5	3.67	3.83	4	4.83	5
Higher management	1	0	0	0	0	0	0	11	5	0	4	0	31	14	0	3	11
Middle management	0	24	16	3	8	17	0	29	0	2	0	18	10	14	1	0	0
Professional/Engineering	0	0	0	0	0	0	10	0	3	24	23	25	50	16	0	0	0

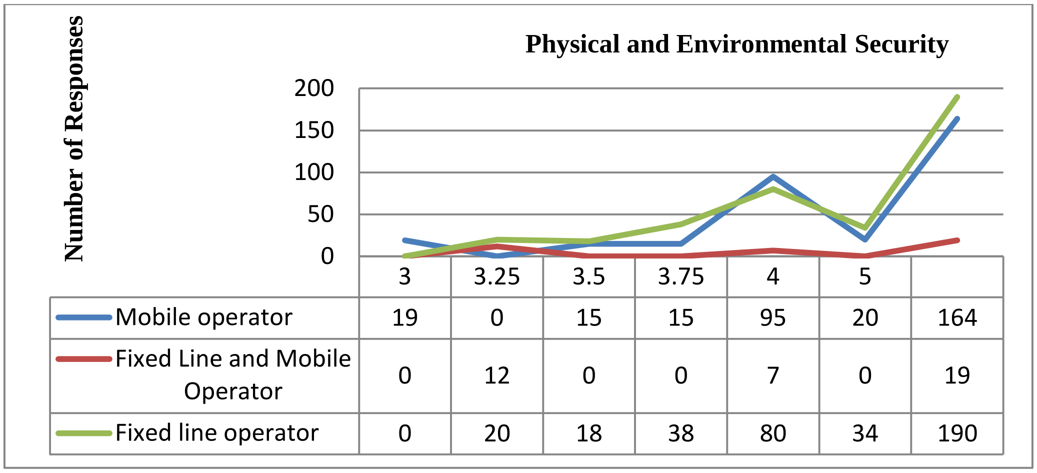
APPENDIX III – Data Analysis - Operator category



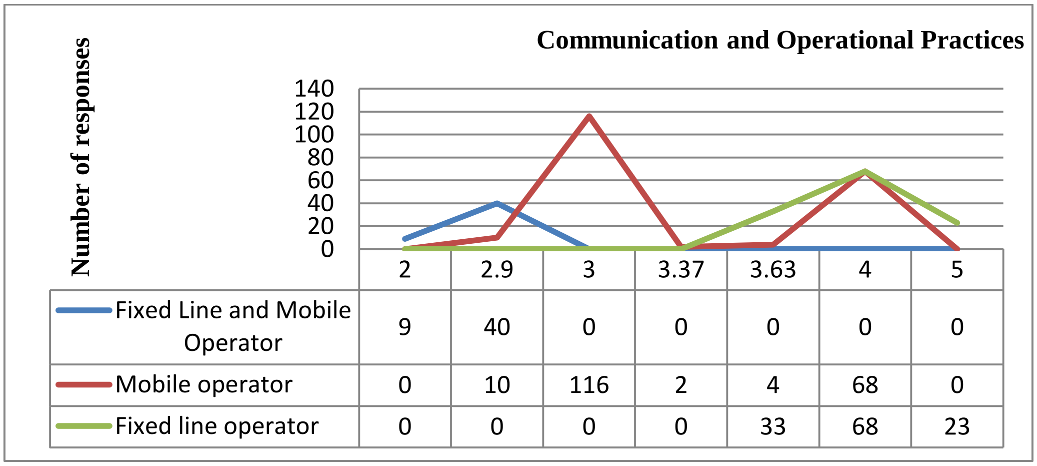
	3	3.17	3.25	3.33	3.42	3.5	3.58	3.75	3.83	4	4.5	5
▬ Fixed Line and Mobile Operator	9	4	6	3	0	4	22	0	0	0	0	0
▬ Fixed line operator	0	0	38	6	0	0	16	0	33	2	9	24
▬ Mobile operator	0	0	1	4	35	29	0	7	0	121	0	0



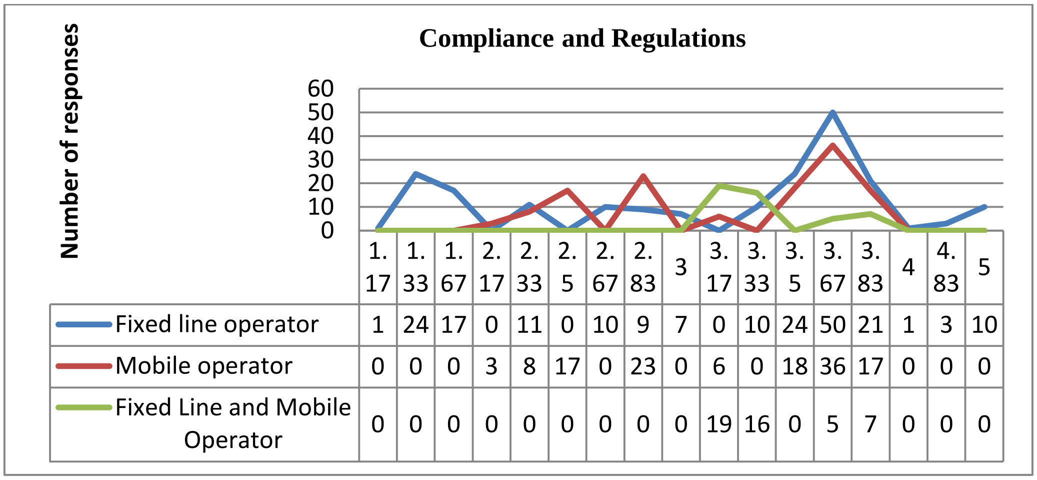
	2.5	3	3.17	3.25	3.42	3.5	3.75	3.83	4	4.5	5
▬ Fixed Line and Mobile Operator	9	4	9	0	45	0	0	0	10	1	0
▬ Mobile operator	0	0	0	57	0	0	7	0	60	10	10
▬ Fixed line operator	0	0	0	0	0	16	0	33	59	19	24



	3	3.25	3.5	3.75	4	5	
Mobile operator	19	0	15	15	95	20	164
Fixed Line and Mobile Operator	0	12	0	0	7	0	19
Fixed line operator	0	20	18	38	80	34	190



	2	2.9	3	3.37	3.63	4	5
Fixed Line and Mobile Operator	9	40	0	0	0	0	0
Mobile operator	0	10	116	2	4	68	0
Fixed line operator	0	0	0	0	33	68	23



	1.17	1.33	1.67	2.17	2.33	2.5	2.67	2.83	3	3.17	3.33	3.5	3.67	3.83	4	4.83	5
Fixed line operator	1	24	17	0	11	0	10	9	7	0	10	24	50	21	1	3	10
Mobile operator	0	0	0	3	8	17	0	23	0	6	0	18	36	17	0	0	0
Fixed Line and Mobile Operator	0	0	0	0	0	0	0	0	0	19	16	0	5	7	0	0	0