Modeling an international organization on information security management and IT security advanced aspects: Model, strategy and organization

Khushbir Kaur Sharma(110894)

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2013

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Modeling an international organization on information security management and IT security advanced aspects: Model, strategy and organization

Khushbir Kaur Sharma(110894)

2013/11/27

ABSTRACT

Now in these days the organizations are using advanced technologies for instance modern cloud, employees bringing their own device at work, use of social networks and resolving borderlines between private and company hours. This is because these technologies are very fast developing, and having flexible and smart features. It seems very clearly that social media have changed the life. For instance face book is often the preferred communication compared to calling on phone or sending email. In case of modern cloud providers fast access to various applications low infrastructural cost has been enabled. Furthermore BYOD enables employee owned devices at work for example smart phones, laptops, I-pads

This thesis work is about to make an educational study platform for the future students related to concepts of modern cloud, BYOD and social media in the modern organizations. For the fulfillment of the author's goal on this research, the author has followed qualitative and quantitative research methodologies. The author has completed his job by defining a case study named CK-TECK for the future students. There author have described the BYOD, Cloud and Social media in the research work which will work as a learning tool for the students. Moreover, the author has described tasks on the topics of Risk Analysis, Information security policies, Risk management according to ISO 27001-27005 and ISACA standards. Meanwhile the author also provided some solutions to the tasks so that the students can take help from those.

The main challenge was to define an open case study framework allowing innovative solutions of new security related threats in advanced technologies. The overall infrastructure of the organization depicts a realistic up to date environment allowing securing it in many dimensions, and presenting in a few cases advanced organizational solutions as well. This case study allows training and education of security management in a completely new and more realistic way, such that future students can work in realistic company like situations.

ACKNOWLEDGEMENTS

I would like to dedicate this whole work to my supervisor Professor Mr. Bernhard M Hammerli. I am highly thankful to him for giving me valuable and right guidance during the tough period of this master research. He helped me a lot by providing me helpful documents and supported me by showing the right direction.

After that I would like to thank my Parents and my Grandfather who supported me for coming in Norway for master study.

I am heartily thankful to the persons who gave me answers of my questions by interviews . The concerned persons are *CSO at Verizon in India, IT Administrator at Velosi in Norway, Senior System Analyst at Accenture in Norway and System Analyst at TCS in USA*

I am also thankful to my loving husband Mr. Chetan Sharma who supported me every time and motivated me so that I can get success for the successful completion of this Master research. He helped me in describing the CKTECK organization together with me. Without his help and support it was impossible for me to start and complete this master thesis research and work. He helped me by giving his creative ideas. He helped me by sorting several problems in the compilation of Latex template too.

With The GOD's Grace and the help of my well wishers, I have tried to complete this Master Thesis(The one of the most important part in my life)

Khushbir Kaur Sharma, MIS Student at GUC, Norway

Contents

List of Figures

List of Tables

1 INTRODUCTION

Information Security Case studies play an important role to understand the realistic view of information security related problems. In these days the corporations are suffering several security related problems because of the emergence of advanced technologies like BYOD, Cloud Services and Social Media. These technologies have been become very important for the organizations in current period. Information security has become an important and challenging issue because of internet. Internet has made everyone's tasks very easy like online appointments, online payments, and online group conversations and so on. On the other hand several securities related issues have been raised too because of advancement of IT infrastructure and modern society. Corporations are very much relying on the advanced technologies of the internet because of their flexible and smart features. Some of the advanced technologies which have been emerged like Smart phones with internet, use of social networking media, Using of Modern cloud network and so on. Corporations are adapting these technologies in these days. An Educational Case study helps the future students to understand the actual problem in a better and appropriate way for the appropriate solution of that problem. This thesis work is all about the advanced technologies (Cloud, Byod and Social Media) in an international organization, the latest and advanced risks in those technologies, Information Security Policies and so on. With this case study the future students would be able to understand the problems of organizations in smart technologies and would be able to develop further solutions of particular problems.

This thesis work is divided into two students i.e. me and one of my peer Mr. Chetan Sharma in initial. My job is to concentrate on non technical aspects of information security in an international organization and Mr. Chetan Sharma is responsible for technical related work (network infrastructure) in the organization. The common part of both students is to discuss about for describe an international organization named "CKTECK", to write history and services of organization, to write job descriptions of several stakeholders, to describe several subsidiaries of the organization, to make an organizational chart, basic risks related to information technology etc. The thesis work is an individual job for both students further. The collaboration of two students is only as discussion for ideas in the starting for describing an international organization named CKTECK.

1.1 TOPIC COVERED BY MASTER RESEARCH

We are living in the advanced world of internet and its related technologies. This master thesis covered the topic of to make an educational case study for future students. This case study is

related to the advanced aspects of information security in an international corporation of 10 subsidiaries. The name of the corporation is CKTECK. The goal of this master research is to design an IT related international organization, its subsidiaries, its services, job descriptions, organizational chart, to describe basic IT related risks in CKTECK, to introduce recent trends in informational technology (BYOD, Cloud and Social Media) used in the organization CKTECK, overall advanced risks related to information security in the organization, current issues of information security in the international enterprises in these days, introducing information security and some of its related policies in the organization CKTECK, future tasks for the upcoming students and so on. The main purpose of the thesis work is to make an advanced case study on (non technical) aspects of information security and its advanced concepts.

In these days technology has developed very vastly and broadly. Several new IT related trends have been emerged in the modern and networked society of today's demand. The role of case studies is to give educational knowledge to the upcoming future students. In the field of information security it is very important to show various problems and advance recent risks so that the students can understand the actual problems and then can find smart solutions to those problems further. Information security is an advanced, latest and new era to be researched further. Therefore the topic of this master research is to model an international organization with several information security management related problems, risks, policies and so on. This case study acts as an educational case study related to advanced aspects of Information Security Management at international level corporation for the future students.

1.2 KEYWORDS

Information Security, International corporations, BYOD, Cloud, Social Media,Information Security Risks, Information security policies, Information Security Management, Risk Management, CKTECK Organization

1.3 CHOICE OF METHODS

The author's main purpose behind this overall thesis work was to make an educational case study platform on the IT security advance aspects, security related hot issues, overall risk management plan in the advance cloud, BYOD and Social Media in modern Corporations for the future students. The BYOD, cloud, Social media has been considered as learning tools for the coming students. These technologies have been considered because these are the latest technologies used in the organizations in these days. In the thesis work the author has developed an organizational based Case Study with advance IT security aspects. This thesis work and research is based on multiple methods and approaches. This is the combination of both qualitative and quantitative research methods. The overall main source of information uses in developing such kind of research was from literatures, organizational documents, recent organizational surveys

on IT security breaches, white papers by several Corporations like ISACA, TCS, SANS. The qualitative method (Interviews with experts,) also helped the author to gain a big knowledge on Information security related advance aspects. The interviews were taken from CSO*Verizon Communications, India*, IT Administrator *Velosi, Norway*, Senior system Analyst *Accenture, Norway* and System analyst *TCS, Chicago, USA* who are working in modern IT Organizations. Moreover the peer student Chetan Sharma, provide his experience and knowledge in defining the MNC(Multi National Corporation), and multi subsidiary Corporation CKTECK.

To make an educational case study for students it is very important to make it with some features like well written, easily understandable by the students, covers the section of basic tasks for the students and some solutions for their help so that they can find solutions on related tasks, some list of potential projects so that they can proceed it in classroom together and individually also and so on. The author tried to cover all this. Therefore she did her work in the following way, which has shown in following Figure 1

1. First of all the author described the basic concepts of cloud, BYOD, and social media technologies in the organizations. These concepts have been described so that the students can learn about these. Moreover these technologies are the recent trends, are the future demands too. The purpose for defining these was to make the students understand these technologies. Moreover tasks for the students are described based on these technologies. For approach this, the author used literature, research papers and interviews answers. Hence it was combination of qualitative and quantitative research. Author found some real and fully conceptualized academic researches so that the author can make concepts from all these research materials. Author has tried to used figures in this section so the students can understand these in a clear way, in depth and in easy approachable way.
2. The next step for the author was to define the Case for the students so that they can read it and can do further tasks. In this the author described an Organization CKTECK with its model and the basic information secuirty policy.This section of creating an Organization CKTECK was followed by using Quantitative (literature, organizations white papers) and Qualitative method (Experts views). That's how the author created an organization CKTECK, with its history, services, customers, departments, subsidiaries and organizational chart with designation, roles of several stakeholders at CKTECK and its basic information security policy. In this part the author presented an idea for the students how to develop a case study for the advance organization. It is very important to have a base model for writing an effective case study. Hence the students can make improvements on it and can take this case study as a base tool, for developing further better case study.
3. Afterwards, the author described some basic tasks for the students on Overall Risk Assessment and Information Security Policy in modern technologies BYOD, Cloud and Social Media. The author created tasks for the students with his own ideas and some help from quantitative and qualitative research for finding organizational related tasks. This also contained author's

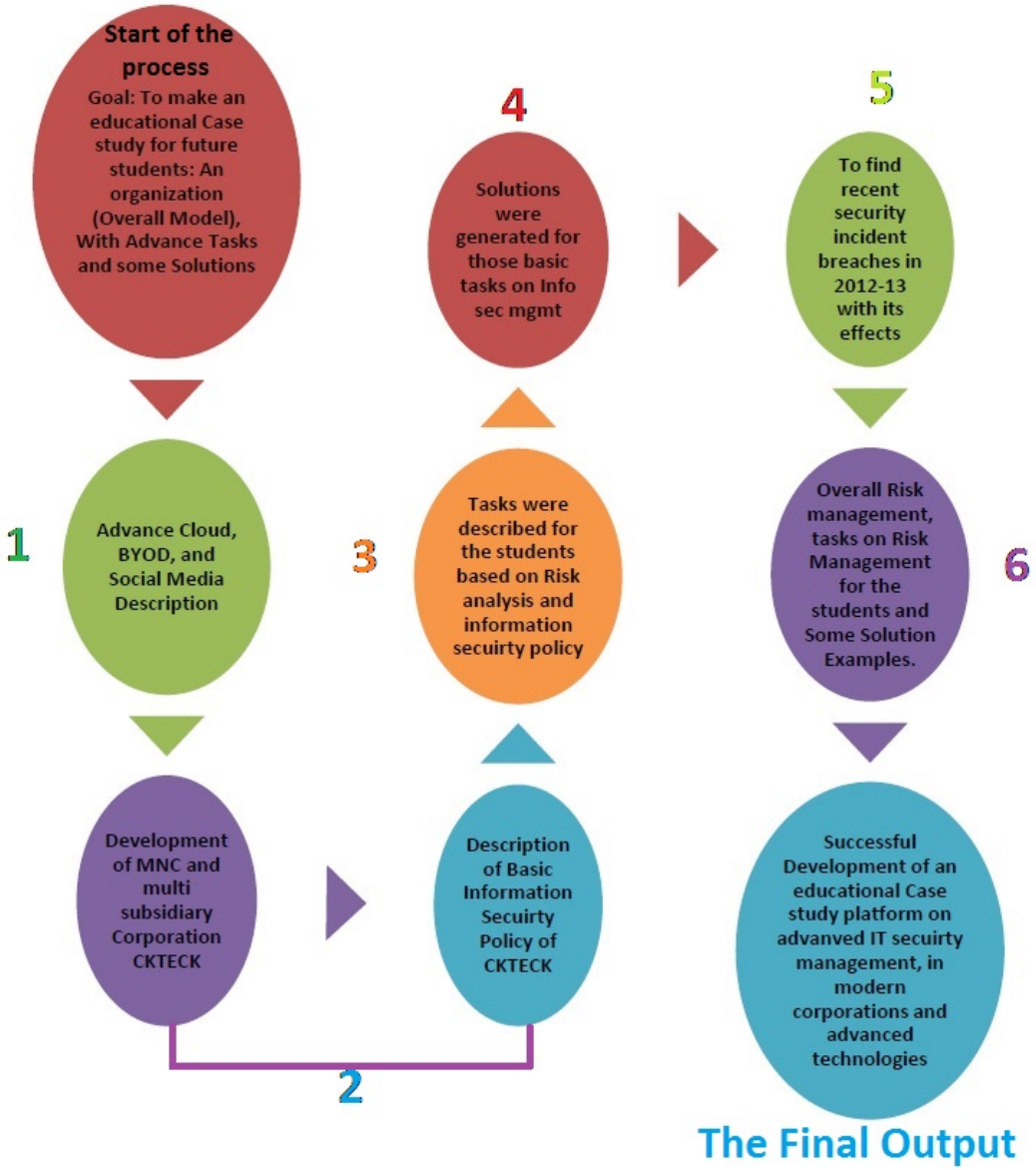

Figure 1: A pathway to achieve the overall concept behind overall Methodology

creativity, ideas, assumptions, views and so on. During the development of case study in previous step, author got some points to generate the tasks for the future students.

4. Next step was to generate the solution material for the students so that they can check their performance. In this section, author followed risk analysis process by finding advance risks in Cloud, BYOD and Social Media according to ISO Standards. Risks are mention in 4.1.2 4.1.2 4.1.2. Furthermore the author also provide solution hint on one of the task re-

lated to the information security policy 4.2. This whole process was done by studying the literature, a quantitative research method plus qualitative research method. This is also based on the output of previous step. In the previous step the author decided tasks, and at this step author produced some solutions for the previous described tasks for the better understanding of whole process.

5. After that the next step of author was to find hot aspects in information security. For this the author used quantitative research. The author found recent surveys of Corporations Sophos, PWC, Websenses, Symantec, of information security breaches in years 2012-2013. The author showed that what had happened and what was the cause of that particular information security incident. This step shows what has done (security incidents) in other advance organizations what was the cause and what was the effect. These surveys have been shown for the students to become more innovative towards the security related aspects.
6. Final step was to develop overall balanced concept for CKTECK's risks. In this the author followed overall risk assessment process according to ISACA and ISO 27001- 27005 standards. The author done frequency/ impact analysis, risk appetite and risk response. The Risk Management tables were produced by the author with her own thinking. Frequency/ Impact analysis done on all risks in CKTECK, Risk Appetite also done on all risks of CKTECK, Key risk indicators were found on some risks as an example for the students, Risk response was done also on some of the CKTECK's risks. This section is also for the students so that they can find the solutions of potential projets which are some further tasks on Overall Risk Management. For this, the author used both qualitative and quantitative research. As a part of quantitative research, author followed ISO and ISACA frameworks for The Risk Management. For finding key risk indicators and proposed solutions the author took ideas from answers by the experts.
7. In the end, the author described the tasks for the students on overall Risk Management and IT security management areas. Students can perform these individually and together in classroom. Description of these tasks was the own assumption of the author as she also has done several projects while studying at GUC, in Msc. In Information Security. This methodology covers the all research questions 1.6 and the related work 2 of this research too. In the end of the process, as a result of this the author got an educational study tool for the future students, on the IT security Management and its advance aspects.

For the overall process, the author tried to concentrate on making an effective case study for the students. For this purpose, the author needed a qualityful work which can help future students in educating them on IT security related advanced aspects in the organizations in recent technologies. The author tried her best to get maximum performance by using several techniques and methodologies. Moreover the author was successful in obtaining every related information for the study tool. In the end of the process the author created a study platform document to the students which may be fulfill the quality of the tool.

1.4 PROBLEM DESCRIPTION

Organizations in a now these days are using advanced technologies for instance modern cloud, employees bringing their own device at work, use of social networks and resolving borderlines between private and company hours. This is because these technologies are very fast developing, and having flexible and smart features. It seems very clearly that social media have changed the life. For instance face book is often the preferred communication compared to calling on phone or sending email. In case of modern cloud providers fast access to various applications low infrastructural cost has been enabled. Furthermore BYOD enables employee owned devices at work for example smart phones, laptops, I-pads etc.

The challenge is to define an open case study framework allowing innovative solutions of new security related threats in advanced technologies. The overall infrastructure of the organisation depicts a realistic up to date environment allowing securing it in many dimensions, and presenting in a few cases advanced organizational solutions as well. This case study allows training and education of security management in a completely new and more realistic way, such that future students can work in realistic company like situations.This master thesis will work as a study platform for the future students in learning about en era of advanced information security, advanced problems of information security, latest realistic and hot issues of information security incidents in the advanced & IT related organizations.

1.5 JUSTIFICATION, MOTIVATION AND BENIFITS

Information security has been become the new demand of the IT related organizations at international level. It is due of the adaptation of recent IT trends like bringing our own devices at job place, adaptation of social media in the organization, adaptation and use of cloud networks and services. Due to the recent demand it is important for the information security students to aware about current problems related to information security in the corporations in these days. Educational case studies plays valuable role to teach a student by describing cases to learn in a better way. Students take the case study as a task and then try to find related solutions on it. This case study will act as an advanced case study to guide and teach the future students about the information security as a new era and its several real risks in the IT corporations in the current time period. Students can read this case study and can work further on it by taking the several information security related problems from it. This case study will provide a realistic view of advanced aspects of information security in organizations in recent trends for instance BYOD, Cloud and Social Media. In this case study the author designed a model of an international organization, advanced information security management risks in recent IT trends. For providing proper knowledge to the future students in the field information security advanced concepts and problems, it is very important to make such kind of case studies. These kind of advanced case studies provide a realistic scenario by which the students can understand the actual problems in a better way rather than just reading. The main goals of the case study have been shown below

1. To describe an international company and the most relevant management structure and processes (The Model)
2. Threats, vulnerability, dependability and risk analysis, according one or several frameworks.
3. Policy for information security management.
4. Overall balanced information security management concept.
5. Task descriptions for students work.
6. Training material (some solution to the task description).

1.6 RESEARCH QUESTIONS

1. What are the recent IT trends used in the international organizations in these days. How to describe an international company with its management structure, subsidiaries, services and processes?
2. What are the advanced information security related risks in the recent technologies in the international organizations?
3. Which are the recent usual and hot issues in the field information security in these days in international organizations?
4. What are information security policies and an examples of information security policy for organization CKTECK?
5. What are the tasks for the future students which can be performed further?
6. What is the example training material that would be valuable for the students to proceed in similar further problems ?
7. How the quality of the tool can be accessed?

1.7 THESIS OUTLINE

Chapter 1provides meta data of the thesis work including basic introduction, problem description, scope, research questions, justification motivation & benefits, methods used for approach of results, thesis outline and so on.

Chapter 2 provides basic introduction of recent IT trends i.e. BYOD, Cloud and Social Media. This is counted as related work because in author's Organization CKTECK, these technologies are used.

Chapter 3 is divided into following two parts

1. CKTECK's Description which includes The Model which includes history, services & areas of products, customers, subsidiaries, the organizational chart, basic information security policy for CKTECK.

2. Task Descriptions for the future students on Risk Analysis and Information Security Policy.

Chapter 4 is about Solutions For the tasks descriptions on Risk Analysis and Information Security Policy which have been described in Section 3.8 of Chapter 3

Chapter 5 is about finding of recent information security breaches in 2012 and 2013 by Corporations PWC, Sophos, Symantec , Websenses.

Chapter 6 shows balanced information concept for the CKTECK. It includes the Overall Risk Management Process by finding, frequency and impact of risks, risk maps, risk appetite, proposed solutions and List of potential projects.

Chapter 7 is about interviews discussions 7.1 ,the future work 7.2 and conclusions 7.3.

In Bibliography, all references have been listed.

In Appendix A, the tables of Risk Management has been shown. In Appendices B C D E all interviews questions & answers have been listed. In Appendix F, abbreviations used in the overall document has been listed.

2 RELATED WORK

The recent trends in Information Technology for instance BYOD, Cloud and Social Media has been changed the lives and minds of the people. These current IT related trends are very smart in nature and provide flexible features and smart functions to the modern society and the organizations too. We are living in the advanced and modern society of internet with several smart and latest technologies of it. Internet and its latest services of new technologies has been become very vast and enhanced, as the time is going ahead. Due to the changing in the time several services have been emerged in the organizations for instance social networking, smart devices as bringing your own devices at work, cloud computing and so on. The organizations are adapting these because otherwise it would be very difficult to be competitive and furthermore it is the demand of the modern infrastructure and society. Therefore the recent advanced technologies [72] which would be considered for latest which are using by the organizations in these days are Cloud, BYOD, Social media, HTML 5, mobile applications. According to the author in [72], these are the emerging trends of 2013. In this master thesis as a case study, the three technologies, which are considered latest are i.e. (1) Cloud (2) BYOD (3) Social Media. Moreover in [70], it has clearly defined about recent trends for instance mobile devices adoption as BYOD, Adoption of cloud providers, Adoption of social media and networking etc. Furthermore ISACA Corporation in [91] describes that the new IT trends in 2013 will be Cloud computing, Mobile computing with cloud and BYOD and Social media as social technologies. The three recent technologies as recent IT trends are described and introduced as a related work.

Related work of this thesis consists of the basic concepts of cloud, BYOD and Social media for some reasons:

- These are the recent technologies of CKTECK
- There are some tasks described for the future students which are based on these technologies
- These technologies are the learning demands for the students because these technologies are the recent IT trends
- Students need to learn these so that they can handle further tasks and problems related to these technologies
- From the learning point to view to the students, it is important to understand the basic concepts behind these technologies
- Students later will be able to understand the problems in these technologies and how to handle these also. They will work as a realistic view in organizations and can how to proceed

with these technologies in the working environment of an organization.

- These technologies can be implemented by the students further, as a development of better case study based on CKTECK's Organization.
- Students also need to find & implement several solutions for different tasks, which are related to these advanced technologies
- Basically these technologies are described in related work so the students can learn on them while they are reading CKTECK and while they are finding risks and countermeasures in these technologies.

2.1 INTRODUCTION TO CLOUD

Cloud computing has been grown continuously from last few years. Cloud computing is very common in the enterprises in these days. From[11], "cloud computing is a new way of offering services" The world of computation has been changed from centralized to the distributed systems and we are getting back to the virtual centralization (cloud computing) [12]. Cloud is a current trend in the organizations and up to 2013 the cloud market is estimated $8.1 billion [31] and $9.5 billion by 2014 [34]. Cloud computing has been used by the organizations as a service infrastructure and cloud computing have different architectures based on different security services of the cloud [12]. Cloud computing can be defined by NIST (The US National Institute of Standards and Technology) in [13] as

"a model for user convenience, on demand network access contribute the computing resources (e.g. networks, storage, applications, servers, and services) that can be rapidly implemented with minimal management effort or service provider interference".From [23], according to the NIST, the definition of cloud is based on following characteristics

- *Users can automatically benefit from the Cloud services without communicating with the service providers.*
- *Standard protocols are used to access the computing resources over the network.*
- *Cloud services follow a multi-tenant model allowing resources to be pooled and shared among users.*
- *Computing capabilities can be quickly scaled in or out based on the users' varying demands.*
- *Users pay for utilized computing capabilities based on a pay-per-use model.*

Another definition of cloud computing from [17] "*cloud computing is an extensive distributed computing standard whereby a pool of virtualized, scalable, vastly available and manageable computing resources (e.g., networks, servers, storage, software, hardware, applications, data) could be*

achieved, utilized and managed with minimal effort"

In cloud computing the programs can be stored centrally and it can be accessed anytime and anywhere even from lightweight smart phones also[36]. From[13], cloud computing is actually a new service which provides a good quality to large scale internet services for the remote applications. Cloud computing is basically used for the sharing of data and computations over around a scalable network of several nodes like data centres, end user computers and cloud services. There are cloud vendors whole provide the cloud services [25]. Cloud services can be provided by one organization and other many organizations use their services [25] for business and other professions as well. Using cloud computing, enterprise could have several benefits because this technology results in increasing the flexibility and scalability [14][15][18][20] of the computer resources even in low cost. In [25], it has explained that Cloud computing is a new computing model which uses public Internet to connect to provider's hosted network, infrastructure, platform and/or applications for provide reliable and flexible services. From [29] there are several benefits of cloud computing. For instance It can give access to large amount of applications and no need of any download.With the help of cloud computing the applications can be accessed from any computer, anywhere in the world. Cloud computing is cheap and avoid expenditure on hardware and software.

The main purpose of cloud computing is to develop a virtualized computing resource pool [30] by centralizing abundant computing resources. These computer resources are connected with network and present the service of infrastructure, platform and software. This network offers various computing resources called "cloud". From [28] *"The objectives of the new computing paradigm are to increase capacity and capabilities at runtime without investing in new infrastructure, licensing new software, and training new recruits. Cloud computing permits customers to utilize cloud services on the fly in pay-as-you-go manner through the Internet"*

Cloud computing is a new paradigm [16], which offers a non traditional computing model to the enterprises to adapt information technology and its other features with low investment. Cloud computing is mixture of new computer hardware with virtualization technologies [19], which is used for the purpose of shared infrastructure which enables web based and value added services. In the infrastructure of the cloud computing the organizations can get cost effective solutions by investing less and by providing less expensive services [21]. Some of the significant features [22], provided by the cloud computing is reliability, scalability, on demand self service, availability to the organizations. Several other benefits [27] provided by the cloud computing are cost-saving, agility, efficiency, resource consolidation, business opportunities and many more. In recent days there are three cloud computing environments[14][17][18][19][21][25][27][30][32][34][35] which are provided by the cloud technology for several different purposes. Figure 2 represents the three computing environments of cloud and their description. Furthermore cloud service models and their examples are shown in Figure 3, Figure 4 and Figure 5

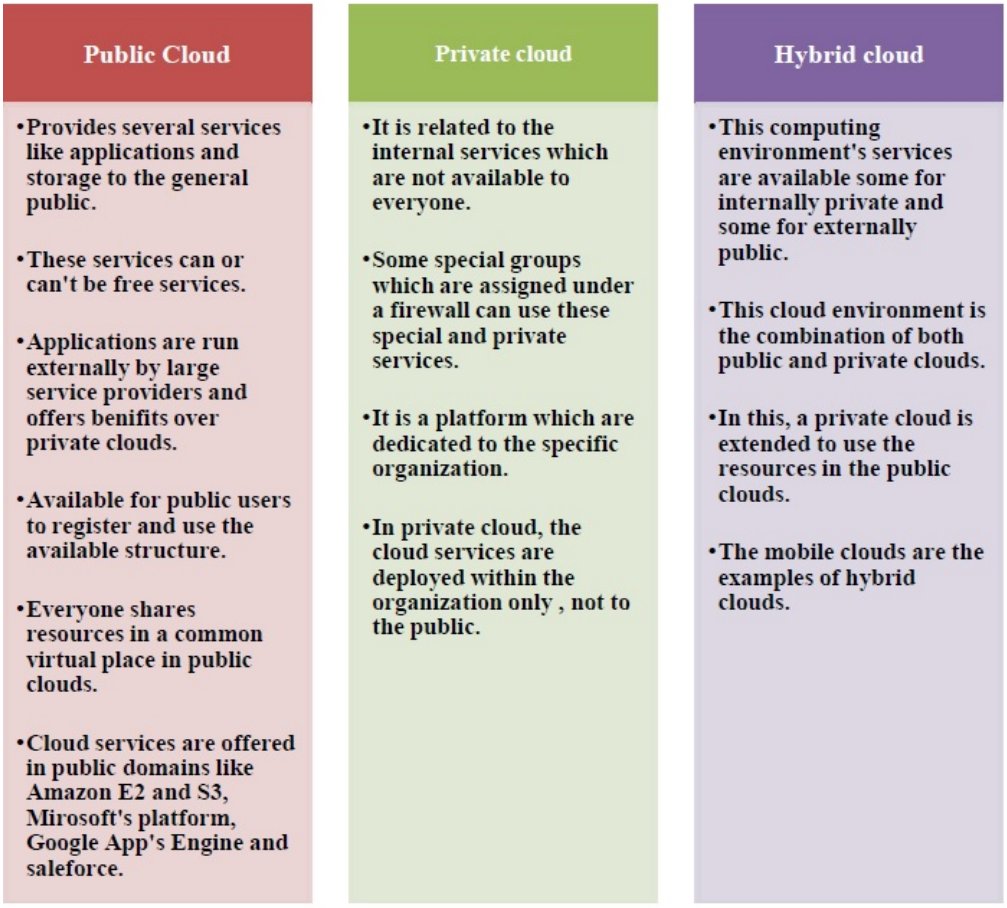

Figure 2: Cloud computing environments public, private, and hybrid (ideas taken from [14][17][18][19][21][25][27][30][32][34][35])

One of the most and recent type of cloud computing environment is the community cloud, [17] [25][27][30][35] which has been emerged also. The most recent cloud computing type "community cloud" and its description has also been explained below. According to NIST in [27] community cloud is*"A cloud which is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission"*

- It is a cloud which is adapted by several enterprises with common interests of them.[17]
- It can be provided by one of the enterprise and used by other group of enterprises in business or professions. These are similar to the enterprise which provides this cloud service.[25]
- The community cloud is the most recent and relevant to The Academic Community like UK

National Grid Service.[27]

- The community cloud can't be classified as public, private or hybrid but it contains the characteristics of all.[27]
- Community cloud starts to work as a private cloud. But because of data sharing requirement it is important to make its service public.Therefore it adds the private cloud services into public domains.[27]
- Community cloud provides the cloud services to the several group of corporations having same missions same challenges same security related aspects and policies.[35]
- Community cloud is cost effective as compared to public, private and hybrid clouds.[35]

2.1.1 MODELS OF CLOUD COMPUTING

Cloud computing models [11][12][13][16][17][18][19][20][27][28][30] are classified into three categories. The name of these three categories of models of cloud infrastructure is listed below:-

(1) Saas, i.e. Software as a service.

(2) Paas, i.e. Platform as a service.

(3) Iaas, i.e. Infrastructure as a service.

DESCRIPTION OF SaaS

- In Saas, the consumers are able to use the applications of the provider's authority. Consumers can use the applications which are running on the cloud infrastructure. These applications are available from the devices on the client side by a client interface for instance web server. Example is Web based emails. [13]
- In Saas, the consumers can use the applications but consumers have no control on the operating system, hardware, software or network infrastructure of the cloud. [17]
- In Saas, software is offered by a third party provider, available on demand, usually via the internet which is configurable remotely. Online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs, etc) are the related examples.[18]
- Saas gives subscribed or pay-per-use users access to software or services which are actually in the cloud and not on the user's device. Saas Consumers application needs thin client software

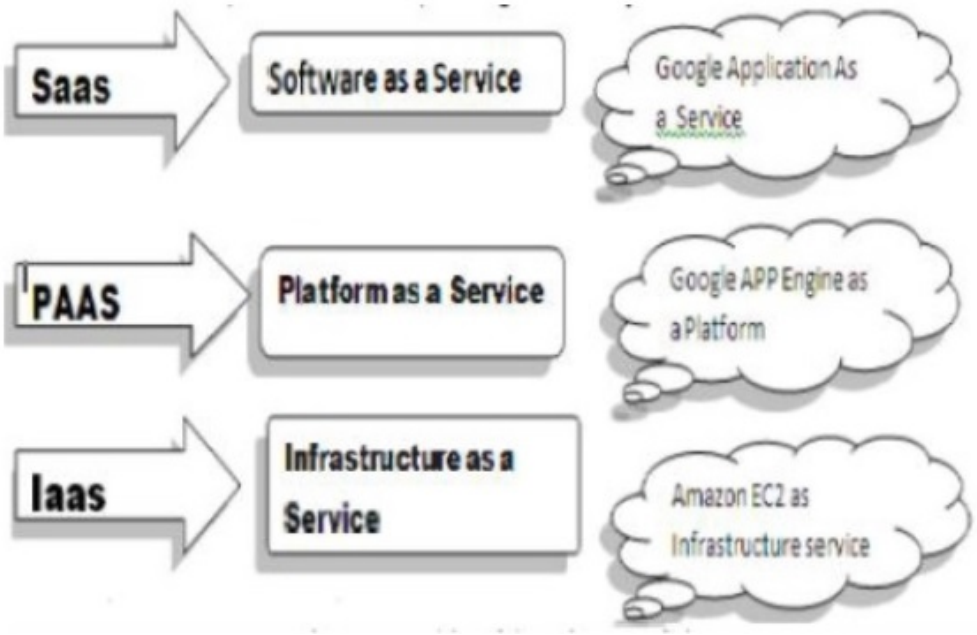

Figure 3: Cloud service models with examples, taken from [13]

such as a web browser which is helpful to access the cloud-hosted applications. It also results in eliminating the hardware requirements for end-users and allows for centralized control, deployment and maintenance of the software. Examples of popular SaaS applications are Hotmail, Gmail, and Google Apps. [19]

DESCRIPTION OF PaaS

- In Paas, the applications, which are created by the consumers, can be put into the cloud infrastructure. Applications can be created by using several programming languages and tools for example configurations.[13]
- Users can build own applications in Paas, which are based on the service providers. Users can control the applications but they have no control on Operating system, hardware or network infrastructure of the cloud. [17]
- Paas allows customers to develop new applications using APIs. The platforms are offered including development tools, configuration management, and deployment platforms. For instance Microsoft Azure, SalesForce and Google App engine.[18]
- In Paas, the consumers are offered a service of developing custom applications like API's programming languages and development middleware, without installing or configuring the development environment. [19]

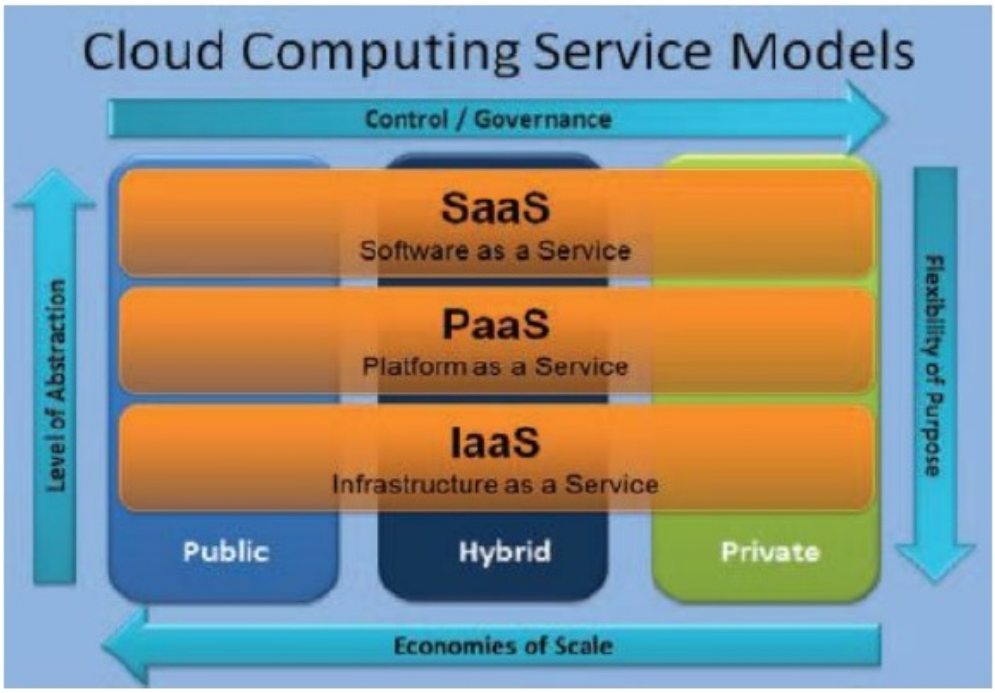

Figure 4: Cloud service models, taken from [16]

- Paas provides benefits like utility computing, hardware virtualization, dynamic resource allocation, and low investment costs. [19]
- In Paas, by using the tools which are included with the cloud platform, developers are able to build applications and services which provides advantages like use of virtualized hardware, data redundancy, and high availability. In Paas, once development is complete, the application can be delivered to the users by use of the Internet. [19]

DESCRIPTION OF IaaS

- In Iaas, the consumers are able to do the provision processing, storage of resources, networking, run software and operating systems for example host firewalls. [13]
- Iaas is the lowest layer of the network. In this, cloud providers can use the fundamental computing resources like processing power, storage, memory, operating system and networking components like firewalls. [17]
- It provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. Examples are Amazon EC2 and S3, Terremark Enterprise

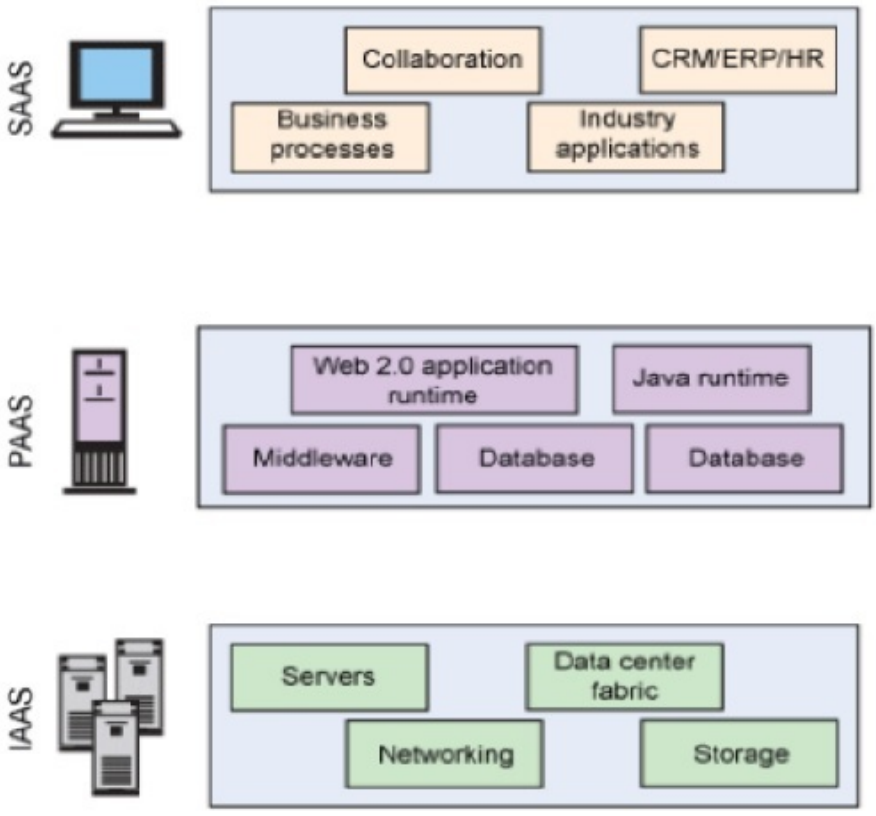

Figure 5: Cloud service models with examples, taken from [17]

Cloud, Windows Live Skydrive and Rackspace Cloud. [18]

- Use of servers, storage, virtualization etc. is provided by Iaas. The infrastructure of cloud in Iaas consists of the facility, communication networks, physical compute nodes, and the pool of virtualized computing resources that can be managed by a service provider. [19]
- IaaS also provides users with a web based service that can be used to create, destroy, and manage virtual machines and storage. [19]

2.2 INTRODUCTION TO BYOD

BYOD stands for bringing your own devices [9] at the work place. BYOD can be referred as BYOT[75] also. It means bringing your own technology that includes both the hardware devices and the software resources. BYOD has become the recent trend in the enterprises because of the development of the smart technologies for instance smart phones, i pads, tabs and so on.Figure 6 shows BYOD Technology in enterprises. From [71], BYOD is a technology under the

concept of consumerization. Consumerization consists of the devices for example Smart phones and Tablets and some smart and advanced services and social media, like Face book, Twitter, Linkedin, DocBox and classical email services. Consumerization from [71], can be described as following.

"The term consumerization describes the growing tendency of the new information technologies to emerge first in the consumer market and then spread into business and government organizations"

By James Hayesin in [74] *the 'bring your own device' proposition is about more than just who owns the computing tool you do your work on followed through to its fullest extent, BYOD could cause changes to enterprise communications provisioning models that have been around for decades*"

Author in[76] says that *"BYOD, or 'bring your own device', is the latest IT buzz acronym. Although the idea's been around for a while, there is a real shift towards allowing employees to use consumer-type devices in the workplace that marks a step change in the way people consume and think of business IT."*

Figure 6: BYOD taken from Google Images

These all concepts are related to the new and advanced services of the modern society of the internet. Internet combined with smart technologies have been changed the world dramatically. Everything has been changed in these days due to the advanced and enhanced media. People have adapted this because it has made the life and lifestyles of the people. Due to the emergence of smart phones, the professionals are allowed to these devices on the workplace for data and applications and their personal use too. According to market research of CISCO from [71], BYOD has been grown up very vastly. Some trends from the CISCO's research[71]] on BYOD upon 600 IT leaders and 18 industries has been described below

- 78 percent of employees have mobile phones at the workplace.
- 44 percent employees are knowledge workers who telecommute at least one day per week with a cost saving of 2500 dollars per year.
- Cloud computing and work shifting technologies have made the BYOD very desirable.

Tom and Beverly in [72] also describes that “The number-one trend affecting today’s enterprise is the blurring of personal and work-related devices”. This is because of the demand of the internet. Enterprises are adapting BYOD to shape the enterprise’s culture, environment and reputation of the IT departments because of demand of modern world and competition in the market. The employees of BYOD can express[80] and dictate the technology they want to use back to information technology. According to Forrester in [80], 33% of us are paying for advanced devices so that these can help us do our jobs in a better way. According to a recent survey by Harris Interactive and ESET in [81], more than 80% of adults which are employed, use some kind of personally owned electronic devices for work-related purposes.

From [73], BYOD has combined with other several technologies for example (1) Development of the HTML-5 browsers, on the mobile devices provides advanced multimedia services. (2) Increasing trend and more adaptation of cloud network and computing itself resulted in adaptation on BYOD. Therefore it seems the BYOD and related technologies are the current and future trend. Even it could be said that the future will be more advanced and attractive.

2.2.1 WHY BYOD

BYOD has been used because of its flexible features and several benefits.Author in [78] explains that "*As a matter of fact, today smartphones and tablets have remarkable hardware profiles and a cornucopia of applications*". BYOD still have some security related issues but its benefits make possible for more use of this technology. Executives are playing a lead role in driving adoption of BYOD in the enterprises [79]. BYOD is attached with the recent technologies like cloud computing and advanced multimedia applications on the mobile phone. Even BYOD seems more comfortable for the employees. Even though, BYOD is the most recent trend for the organizations and this advanced world. For instance, in smart phones like Samsung Galaxy S4, we can run and use several applications like Gmail, Skype, linked in, you tube, What’s app, viber, chat on and so on. So in these days people want to work in an easier way. Because of 3G and 4G, internet is always available on the smart phones. Therefore people started avoiding the use of PCs and started using these smart and advanced technologies. Even these are light in weight, more attractive, more flexible, interesting features, easy to use and carry, all time available. Hence these technologies have made the life easier of the several persons. Some benefits of BYOD from the IBM perspective[87] and MC pc in [88] are:

1. Increasing of productivity in the enterprise
2. More satisfaction in the employees of the enterprise
3. More innovative environment in the organizations
4. With the BYOD costs can be saved by the organizations, because costs are shifting to the users.
5. Results in simplified infrastructure
6. BYOD helps in reduction in ongoing and end user device management, troubleshooting and support.
7. BYOD is very helpful in attracting and retaining top performers.
8. With this, the employee's on boarding and training timings can be reduced.
9. More attractiveness of BYOD provides the competitive advantage to the other persons in the enterprise.
10. By using the employees owned technologies like BYOD, Information Technology teams can focus more on strategic initiatives rather that spending their time on the helpdesk tickets.

2.3 INTRODUCTION TO SOCIAL MEDIA

Social networks are powerful tools that effected the way of life of several professionals. From the literature study in [44], it could be said that social media has become one of the opportunities for organizations to sell their products and services. Enterprises can acquire information about their products and services. By this Organizations can recognize their markets in a better way.

In recent years social media has been got almost a top most position in the modern society and infrastructure. Social networking is a media for people who share common ties that can interact with one another [55]. Social networking has been grown up because of development of attractive and smart social networking tools and their beneficial use. Organizations are very much relying upon the smart technologies and their usage because of advancement and their several benefits. Examples [43] of some common social networking sites are face book, linked in, twitter, orkut, hi5, my space, flicker and so on. From [58] social networking have evolved to be the primary service on the World Wide Web. Figure 7 shows social media example in enterprises. Moreover Figure 8 shows the social media sites examples.

Figure 7: Social Media taken from Google Images

From the author's perspective in [66], *"Social networks empower managers, staff and customers. They don't operate on the same lines as traditional organization structures. They resist dominance, and they erode the traditional, hierarchical power bases in organization. Social networks are surprisingly powerful, perhaps more so than most people realize"* Social networks are powerful tools that effected the way of life of several professionals. From the literature study in [44], it could be said that social media has become one of the opportunities for organizations to sell their products and services. Enterprises can acquire information about their products and services. By this Organizations can recognize their markets in a better way.

Moreover enterprises can get better opportunities to collaborate with their stakeholders. Actually, it has changed the way of life of several. Furthermore we can see that the world has been changed from the time of telegraph telephone to the social networking. In [41] author has wrote that *"with the recent advance of social media and the growing use of social networking tools, organizations are increasingly interested in understanding how individuals, teams, and organizations harvest value from their social networks"*

Steve in [53] gives his views that*"Social networking has made the web a friendlier, more connected but more complex environment. Sites such as Facebook, MySpace, Orkut, LinkedIn and their like have concocted a dangerous cocktail of user-supplied content, open APIs, and web pages heavily loaded with Javascript and embedded media of all descriptions. And it's an environment that is largely devoid of security standards and practices"* From [69],*Social media can be defined as "web-based applications that permit creation, sharing, manipulation and consumption of user generated con-*

tent". Author in [68] explains that "*The use of new electronic media for marketing communication is gaining in popularity with organizations and the adoption of social media*"

Social networking and media has been become the need of everyday's life. Statistics show that social media adoption doubled by U.S. small businesses in 2009 and keeps growing at the time [44]. Face book claims to have a base of over 800 million of active users [58]. It has been reported [44] in 2009 that 93 percent of the participants believe that firms should be present in the social network sites and 85 percent of the respondents think that companies should interact with their customers via the social network sites. Moreover, 64 percent of Face book users have liked at least one brand and it is estimated that 23.1 million users discover new brands or products through social media. As of July 2011, Face book has 750 million users around the world [48] Twitter has 250 million users and LinkedIn has 115 million users. From [61] found that As of February 2012, 66 percent of online adults use social networking sites. From [57] it has been found that Two-thirds of the Internet population in the world are visitors of a social network. Moreover the social networking website has become world's fourth most popular online segment [57]. According to the author of [45], Social networking, micro blogging, etc. are some of the next generation services that have gained prominence. The most recent type of social networking which have been emerged is mobile social networking [51][52]. Many mobile social network applications are available in the market nowadays such as MamJam, Rummble, Dodgeball, Plazes and Jambo [52].

From [61] it can be imagined that up to February 2012, Pew Internet discovered that 66 percent of online adults used social networking Sites. In June 2012, Face book have been attracted 995 million monthly active users and 80 percent users were from the United States and Canada. Social networking sites are the greatest invention and innovation of the past decade and the "best invention of the 21st century" These websites have made significant impacts on the society because they create brand new frontiers for interpersonal communications and interactions. Furthermore these sites have made the society modern and networked.

People are spending large amount of time on social networking sites [57]. There are several needs [42] of the people for instance to be connected every time, to sharing information with friends or others, to become members of the communities, to collaborate and so on. These needs of people are completed very fast and flexibly with the help of social networking. Hence these needs are also a big reason for the vast emergence of the social media and networking. Social media use [42]scalable web based technologies for the implementation of attractive applications. Therefore the social media supports the social interaction. Advanced social media is connected to [42] internet based networking and the virtual environments.

Social networking sites can be defined from [60] as *"Web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of*

*other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. Of course, the nature and descriptive terms applied to these connections vary from site to site.*Social networking websites [43] also called friend-of-a-friend websites. Social media can be connected though these social networking websites. Social networking websites may have several purposes [43] including making friendships, loving romance, collecting information related to business etc.

Figure 8: Social networking sites example from google images

Social networking is based on the communications and connections [43] with other people on the network. Pradeep in [47] explains that social networking sites have been attracted billions of users because of sharing of pictures, images, and communications very easy and fast. Due to the emergence of smart phones the concept of mobile social networking [48] has came. In these days mostly people are used to like communications on the smart phones instead of laptops or personal computers. From [52] web 2.0 services for instance mobile social networking by Apple store has been grouped the applications into following four categories

Mobile front end applications

which are similar to desktop applications like face book and my space. These applications provide trust and sharing only between the friends and these are not applicable for non friends.

Content sharing applications

that allows the users to share the contents like images, files, videos, audios like photo sharing and twinkle to the persons who are friends. These are not available to the users who not friends.

Neighborhood exploring applications

based on location and anonymous interactions. These applications allow users to find, comment, share, and upload multimedia files between users that can become friends.

Mobile specific social networking applications

which are designed for mobile interaction and community. For instance Avatar and Bluepulse mainly focus on the emails and sms communications. Furthermore Loopt and Limbo allows the display of friends locations, activities and making comments about visited locations.

Even social networking applications are integrated into new smart phones [54]. As, the new models are coming the new applications are also emerging in the mobile phone devices. For instance Apple 3, Apple 4, Apple 4s, Apple 5, Samsung galaxy 3, Samsung galaxy 4 and so on. As the new versions of phones are coming, it brings more advanced and smart applications of these smart mobile devices.

3 AN INTERNATIONAL CORPORATION "CKTECK" WITH THE MANAGEMENT STRUCTURE AND OTHER PROCEDURES(THE MODEL)

All organizations expect to protect the confidentiality, privacy and integrity of their employees data. For that it is very necessary for all companies to implement the controls. These controls are needed to balance the nature of the data effectively against the amount of risk involved in accessing, processing, storing, and transmitting that data. CKTECK is an advanced, multinational and multi subsidiary organization. This case study describes the systems, processes, and formal arrangements that have been implemented by CKTECK to ensure the security and privacy of its employees' personal data. The background information and history are explained initially so that it could be understood by the students.

CKTECK is the largest Information Technology software and hardware related organization in four countries of the world i.e. Norway, India, Switzerland, Poland. The Company CKTECK has employed approximately 8,000 people in all subsidiaries worldwide. CKTECK provides several IT related services to its various customers at international level. The services are explained further in the case study. The three main recent IT trends which are used as modern technologies at CKTECK are Cloud, BYOD and Social Media. CKTECK has its own VPN cloud network of each subsidiary and within subsidiaries also. Employees at CKTECK are allowed to use their personal devices at work place for instance smart tabs, I pads, smart phones, personal MAC books, laptops and so on. Employees in CKTECK are using social media and its services in daily routines for the several purposes like message forwarding, video conferencing, audio talk, multimedia sharing and many more. BYOD, Cloud and Social media have become the most popular IT trends in these days and provide more flexibility and modern facilities than the old ones.

From information security point of view there could be several risks and vulnerabilities for the organizations of these technologies. Several risks and vulnerabilities in these modern technologies have been shown in further sections. These risks could be related to the integrity, availability and confidentiality of the information. For instance bringing their own devices at job can arise several problems against CIA of the information. Secret information could be lost if devices are crashed, information can be misused and stolen if the devices are stolen, information can be modified also. BYOD risks may be related to device attacks, advanced malwares, physical access to devices, insider threats, communication problems and compliance related. In case of using cloud, the information can be leaked whenever public cloud is not used safely and securely, information can be misused by criminals and smart persons who can harm the whole enterprise by doing financial loss and reputation loss. Cloud risks may be related to the network security, inter-

face security, data security, virtualization security, governance security, compliance security, legal security at CKTECK. Social media could be harmful for the organization if not used in safe, secure and harmful manner. For instance private information can be visible to outsiders and viruses might be spread into organization's systems. Due to these, information can be unavailable, modified, deleted, misused, and leaked and so on. Social media risks can be related to privacy issues, security issues, trust issues and web threats related issues.

3.1 HISTORY OF THE CORPORATION CKTECK

History of CKTECK belongs to the base of SOCOTEK (software and controller technic AG). SOCOTEK was established in 1980 in Switzerland. Initially the SOCOTEK was developing customized digital hardware. Later on as per the demand modern society organization went into loss. Finally four highly motivated engineers come up with the new digital hardware and software solution. Since 2005 the company has some security solutions for the demand of that time.Now in these days, there is dramatic change in the field of information technology.

When look at the security policies, standards and others security features of SOCOTEK AG, it is based on previous demand and security related risks and threats. It was revised in 2005 and now in these days there is a dramatic change the technology, its demands, its services and so on.From all above, the author of this master thesis come up with CKTECK AG. In which the author developed an advance model of the corporation CKTECK AG according to the current issues in the field of information security. During the work the author covered overall security standards and advanced security aspects of the modern society. CKTECK is an advanced corporation in the field of information technology and information security concerns also.

3.2 CUSTOMERS OF CKTECK INCLUDES THE FOLLOWING MAIN ORGANISATION

Customers of CKTECK includes standardized organization. The organization also take advantage from SOCOTEK AG and able to fulfill the requirements according to the demand. The following organization has been listed below.

- Bank of America (on different locations) bank
- AT & T wireless (Cellular company)
- US cellular
- Comeats
- Cable Connect Inc., Tel Aviv (Israel), Cable manufacturer
- Trossen AG, Honau (Germany) Engineering works

- Weiss & Partners, Goldau (Swiss) Arm manufacturer
- Lotti, Zurich (Swiss) Private bank
- Barmherziges Herz Charity organizations
- Kant. Psychiatrischer Dienst, Zurich (Swiss)
- Vardhman Limited Wool Manufacturer (India)

3.3 FIELDS OF ACTIVITIES AND PRODUCTS

CKTECK is a modern IT organization which has several services. These services are related to hardware, software, communications, BPO, Engineering products, Industrial Design, Virtual effects, Information security and so on. Table 1 provides the clear information regarding the field of activities and products of CKTECK.

Table1

Area	Product	Services
Hardware	• Android smart phone development. • Development of security alarm systems. • Development using micro controllers. • Development of RIFD sensors.	1) The hardware related to smart phone company provides support services to them as well. 2) To the customer when need support about the security alarm related issues than CKTECK AG provides support to them. If there is issue comes in the organisation the alarm on and a signal automatically comes to the provider than again it provides emergency response. 3) CKTECK AG provides the Chip level support to all the customers. 4) Organisation provides the services related to new equipment to be installed at the customer premises. 5) Installation and routine checkups is required for the RIFD than CKTECK Ag provides support services related to these to the customers.
Software	• Relational Database development. • SAP and ERP. • PHP and Java Development. • VC++ and automation. • Python software solutions. • CRM Software development. • CAD, CAM software developments.	After development of the new software the organisation provides support to the customer organisation to install and provide induction to the customer hoe to operate the particular services.
Communication	• LAN, WAN, WLAN, and other communication services. • Cloud based services • VDI services. • Social engineering.	The establishment of the advanced network related infrastructure and technology and security solution related techniques. CKTECK AG provides support services to all their customers.
BPO	• Customer support services • Customer care services. • Technical support services.	In BPO of CKTECK AG it provides customers Telephonic services so that customer can solve their problem over the telephones. if not resolved than raised a formal complaint and resolve by walk-in
Engineering	• Product detailing. • Solid surface modelling. • Finite element analysis. • Reverse engineering.	CKTECK AG provide the services related to detailing of the products Solid surface modelling and etc.
Industrial Design	• Infrastructural management. • Digital design virtualization development. • Technical surface development.	Support services related infrastructure management and technical surface development
Visual Comp Lab services	• Development of visual effects. • Animation development • Development of games.	The VFX technology related service has provided by the CKTECK AG to its customer, development and testing based support provides to its customer.
Information security training services	• General awareness services. • IT and user training. • Technical training. • End user education.	Training and development programme has been conducted the by the various higher level officers and it provides services to the customers companies as well that officer can provide on the job and off the job training to their employees.

Table 1: CKTECK's Areas , Products and Services

3.4 SUBSIDIARIES OF CKTECK

CKTECK is with Ten modern subsidiaries. The four countries are Switzerland, India, Poland, and Norway. The following are the locations of CKTECK Corporation. The description has been shown below.

3.4.1 BULIDINGS IN SWITZERLAND

There are three buildings in Switzerland.Figure 9 shows CKTECK's buildings at Switzerland. Two of them, Altodorf Ost & West, are located at the outskirts of Altdorf at the one side of the Reuss river, while the third building is located on the other side of the river in Attinghausen. The bee-line between these locations is approximately 800 m. The hardware department resists exclusively in Attinghausen, while 95% of the informatics department resist at the two buildings in Altdorf . Some collaborators of the automation department, who are responsible for system integration work at the hardware site.

Figure 9: Three buildings in country Switzerland

The main gate at the Attinghausen area is attended around the clock by a gate keeper. The side is also accessible for trucks, in order to deliver and pick up goods. The employees parking ground is also located inside the area, which is surrounded by a fence and monitored by four video cameras. Robots ready for delivery, large amounts of electronic components, and raw materials are stored in that area. Both buildings in Altdorf have air conditioning, located at the roof of the respective building. The side entrances in both buildings are locked, and are basically emergency exits, though the department chiefs have keys for them. At the main entrance of Altdorf Ost is the secretariat that also functions as a reception.The computer centre is located at Altdorf West. The building is secured via badge and a personal code.

3.4.2 BULIDINGS IN INDIA

There are five subsidiaries of CKTECK in India. The organization contains advanced technologies with newly discovered infrastructure. The locations are situated in both North and south India. In south India the buildings are located in Banglore and Pune. The other three subsidiaries are in the north India i.e. Chandigarh (IT Park), New Delhi and Gurgaon. Figure 10 is about buildings of CKTECK in South India and Figure 11 is about buildings of CKTECK in North India.

BUILDINGS IN SOUTH INDIA

In Pune, there is an office of CKTECK, which is situated in Pune IT park. This building is responsible for making hardware for instance, android smart phone development, development of security alarm systems, development using micro controllers, development of RFID sensors and so on. For the security of this office biometrics system is available. The delivery systems for products are available by using robots. The robots are responsible for carrying the products into the vehicles. Other hardware and software security aspects are also available inside the organization.

In Bangalore, the main area of development is Visual effect computing services. There is a small office situated in Bangalore IT Park. The main activities of the office are Development of visual effects, Animation development and Development of games.

Figure 10: Two buildings in South India

BUILDINGS IN NORTH INDIA

In Chandigarh, the BPO has been established for customer's supports. Customer support services are available for 24*7. For the security point of view they use access card for entering in the office. The employees are allowed to bring their personal devices but they can use them only within the visitor areas. There is an entry system for any unknown person. Moreover the security surveillances are available to monitor each and every activity.

In New Delhi, the building is situated in Information Technology Park. It is a software development area, where so many organizations are situated. There is one office of CKTECK situated in that area. In this building, the software are developed and maintained. This building is responsible for Relational Database development, SAP and ERP Development, PHP and Java Development, VC++ and automation. Python software solutions, CRM Software development, CAD, CAME software developments. This is a small subsidiary of the organization. In this office, there is also an access card system security for each employee.

In Gurgaon, the office is situated in IT Park. This office is responsible for the testing of the softwares, which are made in New Delhi and handling of communication services. The software are checked and verified here at this location for the performance measurement. All communication services are also handled in this building for instance LAN, MAN WAN, WLAN, VDI and cloud etc.

Figure 11: Three buildings in North India

3.4.3 BUILDING IN POLAND

The office in Poland is in Warsaw is responsible for providing engineering and industrial design services. The main services are Product detailing, Solid surface modeling, Finite element analysis, Infrastructural management, Digital design virtualization development, Technical surface development, Reverse engineering etc. Figure 12 shows CKTECK building at Warshaw in Poland country.

(Warsaw)

Figure 12: One building in country Poland

3.4.4 BUILDING IN NORWAY

The main office situated in Oslo. This is responsible for Information security training services such as General awareness services, IT and user training, Technical training, End user education. The main purpose for the building is providing IT security consultancy related services to the customers.Figure 13 shows the building of CKTECK at Oslo in Norway Country.

(Oslo)

Figure 13: One building in country Norway

3.5 DEPARTMENTS AND ROLES

CKTECK has several departments [1] and there are several persons in the organization who are responsible for the maintenance of each department. There are departmental heads also which are responsible for making and assigning duties to the several employees under them. In almost all subsidiaries there are following departments of the whole organization.

1) Finance

2) Legal

3) Human Resources

4) Marketing

5) Sales

6) Product

7) Information Technology (Informatics)

8) Information Security and securities

9) Quality Assurance

3.5.1 FINANCE DEPARTMENT

As clears from the name this department is related to the financial matters of the organization. This department is related to all information and details of funding for the organization. It also contains information about the overall cash flows related to the organization.There are several employees and department heads that are responsible for the maintenance of payable and receiving accounts. In this department, the information related to tax filling also can be found. Other activities regarding this department are the cost tracking for internal and external the organization, budget planning, payrolls, and minimum margins and so on. There records are maintained digital form. There are five CFO (Chief Financial officers) for the finance department for each location of the whole organization. The each CFO is responsible for the related subsidiaries in different countries. There are approximate 100 employees who are working under the CFO's in every subsidiary of the organization. Table 2 provides information regarding financial department at CKTECK.It shows the description of the CFOs for the whole organization's each subsidiary.

3.5.2 LEGAL DEPARTMENT

This department is related to the activities which are related to the legal matters. In other words, this department is responsible for proving and containing the information related to the corporation by laws. Information regarding master agreements according to the laws and rules are also is related to this department. The contracts according to laws and policies, risks, agreements which are purchased rules according to laws, partnerships according to commitments and rules etc. all comes under this department. The insurance claim, losses, licenses problems etc. also comes under the department. For CKTECK there are five main head persons of this department. There are approximate 80 total employees who are working under this department in all subsidiaries of this department. The departmental heads for legal departments are shown in following Table 3.

Table2

Designation CFO(Chief Financial Officer)			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Mr. Pascal Reut Linger	Switzerland	Ost Altodorf
			West Altodorf
			Attinghausen
2	Mr. Rahul Mittal	North India	Chandigarh
			New Delhi
			Gurgaon
3	Mr. Ahmed Khan	South India	Pune
			Banglore
4	Thomas Peterson	Norway	Oslo
5	Ms. Catherine	Poland	Warsaw

Table 2: About several financial officers in CKTECK at different locations of different subsidiaries

Table3

Designation: Head of Legal Department			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Ms. Martin Gerber	Switzerland	Ost Altodorf
			West Altodorf
			Attinghausen
2	Mr. Anshumaan Khurana	North India	Chandigarh
			New Delhi
			Gurgaon
3	Ms. Lilawati Thakur	South India	Pune
			Banglore
4	Mr. Veger	Norway	Oslo
5	Ms. Annie	Poland	Warsaw

Table 3: About several legal department officers in CKTECK at different locations of different subsidiaries

3.5.3 HUMAN RESOURCES DEPARTMENT

This department is responsible for maintaining the human and organizational relations for the corporation. The whole department is responsible for hiring new employees for the organization, firing defective employees from the organization, contracting for the jobs, listening and handling the problems of employees in the organization, helping in development of the carriers of the employees, counseling for employees and so on. There are five HR Managers who are performing

their duties in the organization at different location to maintain the activities of HR department. The following Table 4 shows information regarding HR managers. There are approximate 250 employees who are working for the HR department or the corporation.

Table4

Designation: HR Manager			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Ms. Lucas Gallatin	Switzerland	Ost Altodorf
			West Altodorf
			Attinghausen
2	Mr. Wasim Ahmed	North India	Chandigarh
			New Delhi
			Gurgaon
3	Ms. Puneet walia	South India	Pune
			Banglore
4	Ms. Siv Bente	Norway	Oslo
5	Ms. Hilde Salvoki	Poland	Warsaw

Table 4: About several officers of HR department in CKTECK at different locations of different subsidiaries

3.5.4 MARKETING DEPARTMENT

Marketing department is responsible for maintain the activities like sales and marketing materials, to show the trades, press releases activities, activities related to the market research according to the current period, to do the competitive analysis, activities regarding to the advertising the organization, activities related to the corporation website and so on. The department is also responsible for the publicity of the corporation by using different techniques suitable to current period. There are 5 different marketing heads for the CKTECK and approximate 1500 overall employees who work under the marketing heads. The following Table 5 shows the information regarding marketing heads for CKTECK.

3.5.5 SALES DEPARTMENT

This department is related with the activities which are like relationships related to customers, deal construction, making deals, making projections related to the revenues etc. The department is responsible for the sales and distribution of the products. Moreover, this department is also responsible to introduce the products to the market place. The supply and demand of the product is also depending on this department. In CKTECK there are five main sales managers of this department at different countries and 1000 employees approximately working in the sales department. Description shows in Table 6.

Table5

Designation: Marketing Manager			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Ms. Quentin Swartzendruber	Switzerland	Ost Altodorf
			West Altodorf
			Attinghausen
2	Mr. Ankush Awasthi	North India	Chandigarh
			New Delhi
			Gurgaon
3	Mr. Ankush Khanna	South India	Pune
			Banglore
4	Mr. Andre Hagen	Norway	Oslo
5	Ms. D M Haemmerli	Poland	Warsaw
5	Ms. Jenny	Poland	Warsaw

Table 5: About several Marketing Managers in CKTECK at different locations of different subsidiaries

Table6

Designation: Sales Manager			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Mr. Dario Ankney	Switzerland	Ost Altodorf
			West Altodorf
			Attinghausen
2	Mr. Rahul Mahajan	North India	Chandigarh
			New Delhi
			Gurgaon
3	Ms. Sukhpreet Kaur	South India	Pune
			Banglore
4	Ms. Kathrina Brar	Norway	Oslo
5	Ms. Jenny	Poland	Warsaw

Table 6: About several Sales Managers in CKTECK at different locations of different subsidiaries

3.5.6 PRODUCTTION DEPARTMENT

The product department is related with the activities which comes under for the several products in the CKTECK. In other words we can say that in this department the employees are responsible for converting the input from the output, for instance making products from raw materials. The other jobs of the department are providing requirements for the several products, designing of several products, making pre assumed cost model for the products, cost tracking for the several

products, Development of new products according to new technology, up gradation of already existing products to compatible with the new demands of the society and so on. In CKTECK there are five production managers for the whole organization at several places and approximate 2000 overall employees who are working in this department. The following Table 7 shows information regarding to the production managers.

Table7

Designation: Production Manager			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Mr. Alexender Binggeli	Switzerland	Ost Altodorf
			West Altodorf
			Attinghausen
2	Ms. Megha Sharma	North India	Chandigarh
			New Delhi
			Gurgaon
3	Mr. Chandan Raj	South India	Pune
			Banglore
4	Mr. Knut Veger	Norway	Oslo
5	Mr. Armand	Poland	Warsaw

Table 7: About several Production Managers in CKTECK at different locations of different subsidiaries

3.5.7 INFORMATION TECHNOLOGY DEPARTMENT

In this department of CKTECK, there are 10(ten) IT managers who are the main persons for are responsible for handling this department. The IT managers are responsible for assigning projects to the hardware engineers and the software developers. The network engineers are also comes under this department who are responsible for making and managing organization's network related things. Moreover they are responsible for assigning duties to the employees under them. They are also in charge of measuring performances and checking outputs time to time for the several projects. In CKTECK, there are 1500 approximate employees who work for the IT department in all subsidiaries of the CKTECK. Following Table 8. has information regarding the IT managers of CKTECK.

3.5.8 INFORMATION SECURITY DEPARTMENT

This department is responsible for the maintenance of security of the information and other securities in the organization like physical security etc. In CKTECK, there are five CISO (Information security Officers) persons in several subsidiaries and approximate 200 overall employees who work under this department. The jobs of CISO are making security policies, providing com-

Table8

Designation: IT(Information Technology) Manager			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Mr. David Durian	Switzerland	Ost Altodorf
2	Mr. Rosso Anderson		West Altodorf
3	Mr.Vincent Zwahlen		Attinghausen
4	Mr. Ravikanth Rajput	North India	Chandigarh
5	Mr. Joshanbir Singh		New Delhi
6	Ms. Shama Rajput		Gurgaon
7	Ms. Chandni Khandelwal	South India	Pune
8	Mr Resham Desai		Banglore
9	Mr Andrew	Norway	Oslo
10	Mr J.S Stephen	Poland	Warsaw

Table 8: About several Information Technology Managers in CKTECK at different locations of different subsidiaries

pliance related information, finding security related risks, providing solid risk management, cost and benefit plans for the information security, Transporting the message and educator, Consultant and Advisor, Rescue Conductor, Incident manager, Police Assessor and Auditor, Defining rules of punishment and acts on it, Setting Policies, Guidelines and Standards and so on. Following table shows information regarding CISOs in the CKTECK. There are approximate 100 security guards who work for maintenance of physical security in all subsidiaries. Other persons are responsible for maintain and watching security cameras and so on. Table 9. is all about that information.

Table9

Designation: CISO(Chief Information Security Officier)			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Ms. Julien Frank Heuser	Switzerland	Ost Altodorf
			West Altodorf
			Attinghausen
2	Mr. Anand Sagar	North India	Chandigarh New Delhi Gurgaon
3	Ms. Khushbu Kapoor	South India	Pune
			Banglore
4	Ms. Krithi Stephen	Norway	Oslo
5	Mr. Przemek	Poland	Warsaw

Table 9: About several Information Security Managers in CKTECK at different locations of different subsidiaries

3.5.9 QUALITY ASSURANCE DEPARTMENT

This department is responsible for checking the quality and insurance of the software and hardware products of the CKTECK before the delivery. There are five quality assurance managers and approximate 200 total quality management persons. The following Table 10. shows the information.

Table10

Designation: QA(Quality Assurance) Manager			
Sr. No	**Name**	**Country**	**Place of Designation**
1	Mr Adrian Allen Berger	Switzerland	Ost Altodorf
			West Altodorf
			Attinghausen
2	Mr. Rajat Rastogi	North India	Chandigarh
			New Delhi
			Gurgaon
3	Mr Praveen Tiwari	South India	Pune
			Banglore
4	Mr J.R Gonzalez	Norway	Oslo
5	Mr Januarus	Poland	Warsaw

Table 10: About several Quality Assurance Managers in CKTECK at different locations of different subsidiaries

3.6 ORGANIZATIONAL CHART

Figure 14 shows the overall organizational chart of CKTECK. CKTECK have several stakeholders who have their different positions according to a level. The organization chart flows from top to down for instance from highest to lowest positions at enterprise CKTECK. This chart shows the positions of all stakeholders at CKTECK in its all subsidiaries.

3.7 ROLE OF INFORMATION SECURITY POLICIES AND INFORMATION SECURITY POLICY FOR CKTECK

As concerning important to the term information security, many organizations have started to implement ISO standards, NIST standards, Federal Information Standards etc [83]. It is because to pay attention in the security of the valuable information of the organizations.Any Policy [83], can be defined as a guideline, a procedure or a standard. But actually it is different from all three terms.

> “A guideline can be defined as suggestions for the best way to accomplish a specific task”

> “A standard is a minimum requirement in order to comply with the policy. They are derived

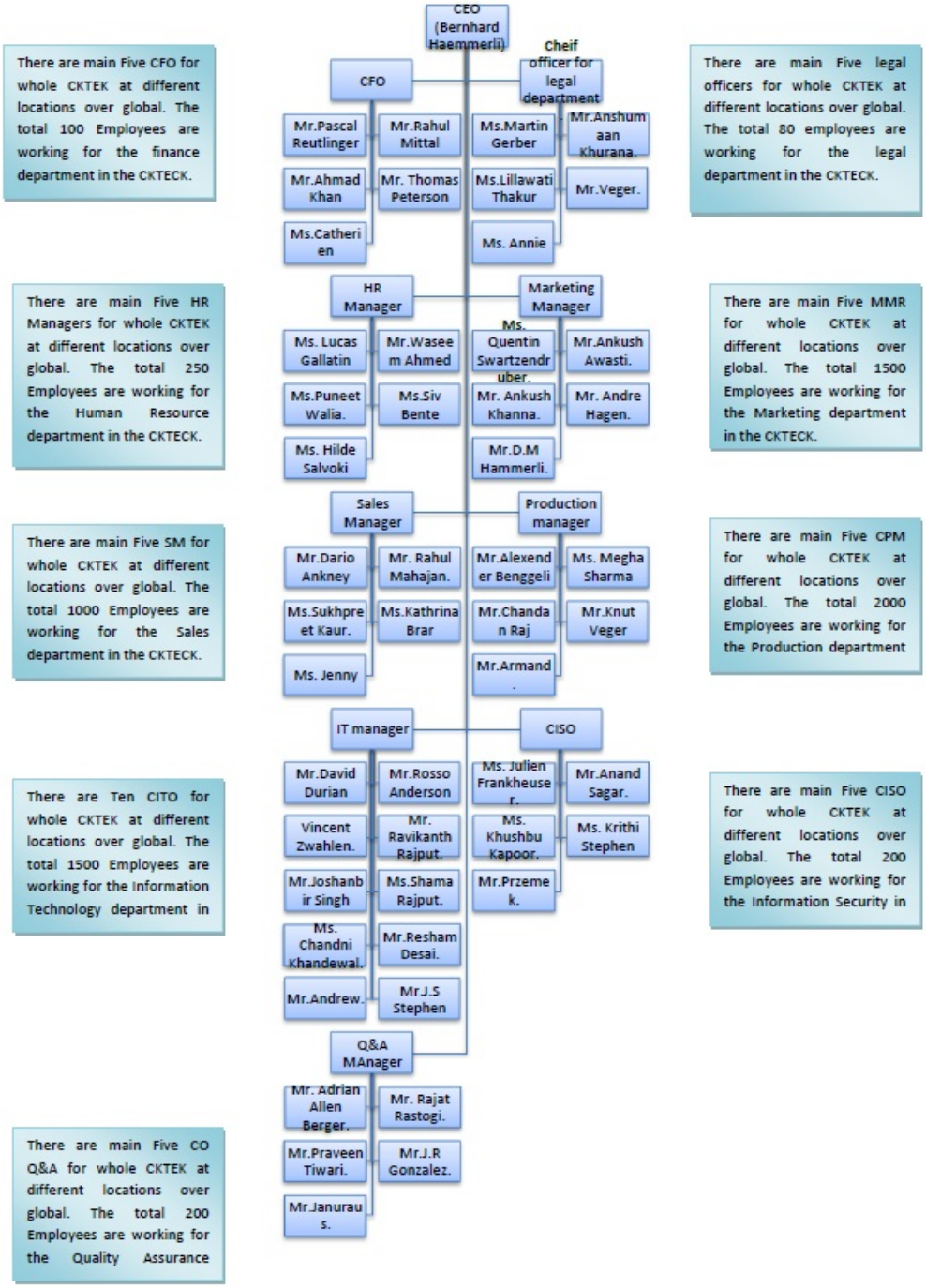

Figure 14: The organizational chart of CKTECK

> from industry best practices, experience or organizational drivers. They must be reviewed on a regular basis to ensure that they are still relevant or to address any new vulnerability."

Security standards provide guidance towards achieving specific security policies, often related to particular technologies or products. They are used as a benchmark for audit purposes and are derived from CKTECK's best practices, experience, business drivers, internal testings and so on.Standards should be reviewed regularly address the ensureness new releases and vulnerabilities. Examples of standards could be UNIX server builds, firewall configurations, connectivity protocols.[89]

> "A procedure can be defined as a method by which a policy is accomplished. They must be clear, tested, documented as well as reviewed and updated on a regular basis"

Examples of procedures [89] are reporting incidents in the CKTECK, Management of CKTECK's incidents, addition/removal of CKTECK's user ID's, server backups and many more

Information Security Policy for the Corporation CKTECK will explain the responsibilities of stakeholders and other individuals in CKTECK, who are responsible for access the technology systems in CKTECK. Some of the following items [83] could be a part of CKTECK's information security policy

- How access to computer systems at CKTECK will be given and maintained
- How to properly use of CKTECK computer systems
- How to respond to a security incident In CKTECK
- What legal and regulatory obligations are involved with CKTECK

Some of the examples of specific CKTECK policies [89] [90] are listed below

- CKTECK's Information security policy
- CKTECK's Information classification policy
- CKTECK's Access control policy
- CKTECK's Communications and Operations Management policy
- CKTECK's Incident management policy
- CKTECK's Physical and Environment security policy
- CKTECK's Human resources Management policy
- CKTECK's Third-party access Management policy

- CKTECK's Business continuity Management policy
- CKTECK's Network security policy
- CKTECK's Disaster Recovery policy
- CKTECK's Information security policy
- CKTECK's RISK management policy
- CKTECK's Compliance related policy

3.7.1 WHY INFORMATION SECURITY POLICY

There could be several reasons that why CKTECK needs an information security policy.

- To make successful many items of Corporation CKTECK to its several departments, processes and customers [83]
- To protect the CKTECK from vulnerabilities and attacks[83]
- It helps in reducing ambiguity in CKTECK [89]
- It provides agreed roles and responsibilities for several individuals of CKTECK [89]
- To aware CKTECK from new security related threats

3.7.2 CKTECK'S INFORMATION SECURITY POLICY(PRELIMINARY AND BASIC)

The information security policy document for CKTECK organization will contain several sections . It will explain the rules, responsibilities for several stakeholders at CKTECK. CKTECK's overall information security policy document will explain the purpose and scope for it, its objectives, Important definitions, Information Assets, Information Security Principles, General Responsibilities for several stakeholders of CKTECK. The sources from which the author has taken help and ideas to produce an information security policy for CKTECK Corporation are [83], [82], [24], [84], [89], [90], B

ABSTRACT

CKTECK's information Security policy contains the principles and guidelines which can be applied for the protection of the information of The CKTECK Group and its all Business Units and legal entities respectively. It would be applied to that information also which is transmitted between the BU's/legal entities, The CKTECK Group and the outside world. This policy will directly apply to all Employees of the legal entity of The CKTECK Group. Additionally, it will define the

minimum requirements, which the relevant policies on Information Security of The CKTECK Group's BU's and legal entities shall satisfy.

PURPOSE

The Executive Board of The CKTECK Group is committed to ensuring that The CKTECK Group, its BU's and legal entities are conducting their activities in such a way that information assets are adequately safeguarded from potential security threats. This policy describes the principles, which apply in order to protect the information held by The CKTECK Group and its BU's and legal entities respectively and transmitted between the BU's/legal entities, The CKTECK and the outside world. These principles are designed to take into account the value of information for the Group as a whole, including the relevant legal and regulatory obligations and good practice in the financial sector.

SCOPE

This policy covers all information, which is stored, processed, transmitted or printed using any system and storage medium. This directive shall apply directly to all Employees of the legal entity of he CKTECK Group. Moreover this policy shall define the minimum requirements, which the relevant policies on Information Security of CKTECK Group's BU's and legal entities shall satisfy. The CKTECK Group's BU's and legal entities shall implement the minimum requirements which are contained herein through the adoption or revision of their own policies and guidelines on Information Security, taking into accounts the relevant local laws and practices.

OBJECTIVES

Information security is a prerequisite for the long-term existence of The CKTECK Group and its BU's. The secure handling of information requires the careful co-ordination of technical and organisational measures.

The objectives of information security are:

- To ensure that all information is protected against unauthorized access.
- To ensure that all information is adequately protected against corruption or loss during input, processing, transmission or storage.
- To ensure that all information and information systems which are essential to the conduct of CKTECK Group activities are adequately protected with respect to the level of IT services required.
- To create and maintain awareness of the need for information security as an integral part

of the day to day operation of business systems. This ensures that all Employees of CKTECK Group understand the importance of information security, their own responsibility for security and the effects of security upon the success of the whole CKTECK Group.

- To ensure that all Employees are aware of and comply with relevant internal and external rules relating to the maintenance, protection and withholding of information.
- To ensure that secret information of The CKTECK Group should not be misused by the employees of The CKTECK Group.
- To ensure CIA(Confidentiality, Integrity, Availability) and AAA(Authorization, Authentication, Accounting) of information security of The CKTECK Group.

DEFINITIONS

- "Business Unit" or "BU" means each business unit through which the the whole CKTECK Group is operating its banking and/or insurance business. Business Units may be counted as Financial Services of the CKTECK.
- "The CKTECK Group" or "TCG" means the ultimate holding company of the Group, i.e. the parent company holding participations in any subsidiary, directly or indirectly, 50% or more, or in any other company, for which it has the right to elect a majority of the Board.
- "Employees" means, for the purposes of this policy, full-time and part-time employees as well as temporary employees and shall include, but not be limited to, consultants and contractors as well as members of the Executive Boards and the BU's Executive Boards (Executive Boards of individual Business Unit)
- "The Group" means CKTECK'S Group and any subsidiary held, directly or indirectly, 50% or more by The CKTECK Group or any other company, for which CKTECK Group has the right to elect a majority of the Board, or any Business Unit or division of CKTECK group.

INFORMATION ASSETS

Information is a vital asset to the whole CKTECK Group. Information is used in every aspect of the Group's business. The CKTECK Group and its BU's are heavily reliant on IT for the storage, processing and presentation of information. As a result, The CKTECK Group is dependent on the control of information being fed into its computer systems and on the functioning of the computer systems themselves.

PRINCIPLES OF INFORMATION SECURITY

There are some principles of information security. Information Security principles can be defined as CIA (Confidentiality, Integrity, Availability), AAAA (Authentication, Authorization, Accounting, Access Control) [24] and some of the further aspects like Audit Trials, Cost and Residual Risks, Risk management and Information Security Economics, Documentation, Maintaining Information Security.

CONFIDENTIALITY

Confidentiality means to hide the secret and private information of the CKTECK Group from the unauthorized access of any third person and from all unauthorized persons.

INTEGRITY

Integrity means to ensure that the information of CKTECK Group should be correct and not modified by unauthorized persons outside from the CKTECK. In other words, integrity of information means it should be secure enough that only employees within the CKTECK should have access to modify it.

AVAILABILITY

It means that the information should be available when it is required by the employees of The CKTECK Group. It should not be deleted, destroyed or corrupted by the persons which are outside from the The CKTECK Group.

AUTHENTICATION

It means that only legitimate users of The CKTECK Group can access the information with some certain credentials. Others should not have right to access the secret information of the CKTECK Group.

AUTHORIZATION

Authorization means that the information should be restricted amoung the several employees in The CKTECK Group. The information related to financial matters of CKTECK is restricted to show to every employee in The whole CKTECK Group. It should be visible only to the financial managers and finance departments.

ACCOUNTING/AUDIT TRIALS

IT related processing must be traceable by the responsible persons of The CKTECK Group by means of the logging of relevant information. The audit trail should allow checking of the validity of information sources and any changes made.

ACCESS CONTROL

Access Control is the process of controlling access to systems, networks, and information which is based on business and security requirements. The objective of Access Control is to prevent unauthorized disclosure of the whole CKTECK Group's information assets. For instance identification, authentication, and authorization. This applies to the people, process, and technology devices within the whole CKTECK Group.

COST AND RESIDUAL RISKS

Information security measures must adhere to cost/benefit principles. Any remaining risk must be brought to the attention of senior management of The CKTECK Group. This will ensure that residual risk is within acceptable limits.

RISK MANAGEMENT AND INFORMATION SECURITY ECONOMICS

Risk Management process in monetary terms with information security economics should be done carefully by the responsible hired employees of the CKTECK Group. The results must be visible and shown to the higher authorities in The CKTECK Group.

DOCUMENTATION

Details of the scope and level of information security measures implemented must be documented in a complete, clear and up-to-date manner.

MAINTAINING INFORMATION SECURITY

Information security must be constantly reviewed, updated and adapted in line with changing conditions and technology, while taking into account changes in the level of risk and in security mechanisms.

GENERAL RESPONSIBILITIES

BASIC PRINCIPLES

- Information security is not simply only an ongoing managerial task. It is also the responsibility of each and every individual Employee.
- For reasons of responsibility, Group data which need a certain protection level must have a designated 'owner'. Owners are responsible for their information and, in particular, for its classification.
- The primary responsibility for protecting information assets lies with the management of The CKTECK Group and the respective BU's respectively.

EXECUTIVE BOARDS OF THE CKTECK GROUP

The Executive Boards of CKTECK Group is responsible for endorsing and supporting the Group information security policy and for ensuring that information security retains a high profile within the Group.

EXECUTIVE BOARDS OF INDIVIDUAL BU's (Individual Business Unit's Executive Boards)

- The every Executive Board of each Business Unit in CKTECK Group will approve major initiatives aimed at enhancing information security and will guarantee that resources are available for the ongoing development, implementation and review of appropriate regulations.
- Every BU must appoint a Chief Information Security Officer who will be responsible for setting BU policies and standards.

CHIEF INFORMATION SECURITY OFFICERS B

- a)The Chief Information Security Officer (CISO) within TCG and each BU is responsible for setting out and publishing policies and standards, for providing advice and guidance, for monitoring compliance, and for the co-ordination of the effort required to attain security objectives.
- b) The Chief Information Security Officer (CISO) within TCG and each BU is responsible for security of information and Data processed in the org.
- c) The Chief Information Security Officer (CISO) within TCG and each BU is responsible for to have information security group to manage all exceptions.

- d) The Chief Information Security Officer (CISO) within TCG and each BU is responsible for to do continuous risk management and ensure sufficient security controls on systems.
- e) The Chief Information Security Officer (CISO) within TCG and each BU is responsible for defining and reviewing and cascading security policies to one and all.
- f) The Chief Information Security Officer (CISO) within TCG and each BU is responsible for Governance, assessment of security health poster in the org via periodic internal audits.
- g)The Chief Information Security Officer will be responsible for any investigations regarding breaches of Information and IT security and for the subsequent implementation of appropriate measures. This includes joint responsibility for cross BU coordination.

LINE MANAGEMENT

Every line manager within TCG and its BU's is responsible for ensuring that good security practices are implemented and maintained within their area of responsibility by:

- Ensuring that Employees know what is expected of them and act in a sensible way to protect information and information systems.
- Maintaining awareness of the risks associated with the loss of confidentiality, integrity or availability of information.
- Encouraging all Employees to raise potential security issues with their line manager or with Information/IT security.
- Setting a good example for staff by taking the lead in applying good security principles to their own work.

OTHER EMPLOYEES

- All Employees within The CKTECK Group and its BU's are required to safeguard the information, which they create, receive, or control.
- All Employees are required to notify their line manager, Information/IT security or the security staff, as appropriate, with regard to any Information/IT security-related incident or issue, which may arise.

3.8 TASK DESCRIPTIONS FOR STUDENTS

In initial, future students have tasks on the two main areas that has been listed below

1. TO DO RISK ANALYSIS
2. TO DEFINE SECURITY POLICY

3.8.1 TO DO RISK ANALYSIS

Students have to find overall risks for the CKTECK , a multi subsidiary and an international organization. After careful reading of the company's description students can find risks in several departments of CKTECK. The modern and recent IT Trends should be considered as the areas for finding risks. There are further two tasks for the students which come under Risk Analysis.

1. RISK IDENTIFICATION

2. FINDING COUNTERMEASURES

In 1st Task Risk Identification, the students need to identify several risks in different departments of the CKTECK. Students should find at least 30 risks related to integrity, confidentiality and availability of the information in case of using BYOD, Cloud and Social Media in the enterprise CKTECK.

In 2nd Task, Finding Countermeasures, the students need to find at least two countermeasures for each risk.

THREAT PICTURIZATION

The Threat Picture is very advance. It is according to the advance aspects of information security and modern society. There are several problems in the modern technologies for instance

- The criminals have taken higher education and even the criminals are going to become very smart. They are using modern hacking techniques and they are also intelligent persons.
- There are more goal-oriented attacks and fraud. Examples for frauds are data theft automatically from accounts of employees. Stealing secret information of company and then misuse it.
- ID-theft and blackmailing are also a main concern in these days. Hackers or criminals can

steal user ID's and then can blackmail to the organization's employees for the purpose of stealing money. Criminals can also damage the company's reputation.

- Botnets and trojans are for a purpose of data theft. These are very smart and send by intelligent criminals. These can make fool to the employees and can steal secret data of company. These can also result in system failure or crash.
- New viruses and distribution are also emerging as the growth in new technology.
- Hidden techniques can be used by intelligent bad persons which can harm the overall organization.

STORAGE MEDIA FOR INFORMATION

The storage media for the information could be any from the advanced and modern technology. Some storage media device from the advancement are Personal or Organization's Apple I-Phones, Personal or Organization's Samsung Galaxy 4 Smart Phone, Personal or Organization's Apple or Samsung I pads, Personal or Organization's Laptops, Personal or Organization's Samsung or Apple Tabs, Personal or Organization's Flash Drives, Personal or Organization's Moveable Hard Drives and so on.

THREAT CHALLENGES FOR RISKS

Some threats and challenges for the risks are shown in the following list

- Moveable Tele Workers
- Third Party and Outsourcing
- Confidentiality
- Availability
- Auditing
- Stolen Devices
- Memory Sticks
- BYOD Challenges
- Training And Awareness
- Personal and Secret Data
- Cloud Challenges
- Use Of Facebook, Twitter, Linkedin, Skype, Youtube

- Seurity Policy

RULES FOR TASK 1

Some rules for doing Task one are shown below.

- Find and identify at least 30 risks for overall departments and advanced technologies in CKTECK
- Describe the risks in two to three lines so that these can be understood easily.
- Find how to save from such kind of risks and what the possible minimum two countermeasures for each risk. Countermeasures should be related to IT Solutions for the organization.
- Work in two or three students group.
- Try to work as a feeling of an interesting task. Don't feel hectic. Take it easy and relaxing and think yourself as working as a "Risk Analyst"
- Risks should be found by using ISO 27001-27005 standards, ISACA RISK IT Framework Practionary Guide, COBIT and so on. Risk Assessment can be done according to following domains under ISO 27001-27005 [5].

    - 1) CKTECK's Management (Security Policy)
    - 2) CKTECK's Security and Safety Organization
    - 3) Assests Classification and control in CKTECK
    - 4) CKTECK Personnel Safety and Security
    - 5) Physical Safety Security and Environment of CKTECK
    - 6) Incident Management in CKTECK
    - 7) Network security of CKTECK's network infrastructure (WLAN between sites, local area networks)
    - 8) Development and maintenance of systems or Computer and network management in CKTECK(security of premises)
    - 9) CKTECK's Logical access control system
    - 10) Information Technology and Information Security of CKTECK
    - 11) CKTECK's Legal and Compliance matters
    - 12) CKTECK's Application Security and Cryptology
    - 13) Business Continuity and Recovery Planning In CKTECK

3.8.2 TO DEFINE SECURITY POLICY

Task 2nd for the students is related to the security policy for the information security purpose in CKTECK. Suppose you are hired as a CISO (Chief Information Security Officer) in the CKTECK. A very basic security policy has defined in the description of CKTECK. Moreover basic roles of CISO have been shown in the security policy. You need to find solutions as a role of CISO, that what would be your roles and responsibilities for CKTECK organization at several areas and departments. There are some questions listed below.

TASK 2nd QUESTIONS

1. What kind of Access Rights and Passwords should be used for the secure environment of CKTECK Corporation?
2. What kind of information security policy related terms and conditions for the internet and email services for the CKTECK?
3. As, considering yourself a CISO in CKTECK how will you be able to maintain the security policy management? How can you create, issue and maintain CKTECK's information security policies, standards, guidelines, processes and procedures?
4. How can you organize a smart information security management program in CKTECK as a CISO? What should be your role of in CKTECK's secure IT Governance, CKTECK's third party agreements, CKTECK's non disclosure agreements etc.
5. How can you do protection and management of CKTECK's Assets? You need to define about how can you be responsible for protection of CKTECK's assets and classification of information for several employees at CKTECK?
6. In case of CKTECK's Human resources Security & CKTECK's Environment and Physical security, what are your main responsibilities as a CISO? You need to find your creativity and duties in case of physical security at CKTECK and Environmental security (heating, water and air) at CKTECK. You need to define your roles in Human Resources Security like screening processes at CKTECK, Information security management training and awareness at CKTECK, change or termination processes in employment at CKTECK, Removing of access rights after leaving CKTECK, Return of CKTECK's assets and so on.
7. How the Communications and Operations Management of CKTECK's can be managed securely by you as a role of CISO in CKTECK. How can you responsible for

    - Document operating procedures at CKTECK
    - Providing Protection against malicious and mobile code at CKTECK
    - CKTECK's Backup functions.

- CKTECK's Network security management.
- CKTECK's Media handling
- Exchange of information at CKTECK
- CKTECK's Electronic messaging.
- Electronic commerce services.

8. What are the several access control rules and mechanisms for CKTECK's protection from a CISO's point of view? What would be your role in network access control, OS access control, application and information access control, mobile working and teleworking access control?
9. In case of any information security incidents in CKTECK, what are your plans and actions as a CISO in CKTECK? You need to define at least five information security incidents at advance and modern international CKTECK enterprise. You also need to write your pre, during and post incident plans in case of information security incidents. Moreover what would be your try in handling such kind of incidents?
10. If there will be any natural disaster at any of CKTECK's Location, for instance in Switzerland, then what will be your duties as CISO at CKTECK. How will you try to recover from floods or fires? What would be your pre, during and post disaster recovery plans for CKTECK?
11. In case of internal and External Compliance of CKTECK, What would be your planning and roles for executing a secure information security management program? List your possible roles in this field as a CISO at CKTECK.
12. The several types of information security policies which are listed on Page 39 and 40, can you write two of them. You can write on any two types of advanced information security policies (For example CKTECK's Access Management Policy, CKTECK's Disaster Recovery Policy etc.) for the organization CKTECK.

RULES FOR TASK 2

- Students can work in group of two. Each student should find at least 10 minimum rules and duties in case of any two areas listed in the questions. Therefore two students must take at least two questions in a group. After that they can find solutions individually and then combine their different solutions with each other. Finally the two students in one group can make one report with combined solutions.
- Students can take help from Information Security Governance Programs like NIST Guidelines, ISACA information security guidelines, COBIT information security guidelines, SANS Institute Guidelines and so on. But the duties and roles should be adjustable in the CKTECK's environment.
- Students should not feel bounded. They must do the tasks as a feeling of CISO at CKTECK and can give their suggestions too. But it should be related to CKTECK's problems.

4 SOLUTIONS MATERIAL TO STUDENTS

This chapter will provide information regarding the solutions on the tasks of risk analysis and information security policies in CKTECK. The risks are related to the overall risks in advanced technologies BYOD, Cloud and Social Networking usage.

4.1 SOLUTIONS FOR TASK 1 i.e RISK ANALYSIS FOR CKTECK

Risk Universe [2] means the overall every type of risks in the organization according to the different departments in the organization. There are several risks in different departments for the whole organization CKTECK according to the changes in the technologies and adaptation of new demands of the modern society. CKTECK is actually a modern and advanced organization which is adapting all of the new technologies for instance use of social medias, modern cloud network, brining the own devices at jobs and so on.The several areas [3] [4] of organization CKTECK, are listed below. In these areas, several risks can be assumed related to Advance Cloud, BYOD and Social Media.

4.1.1 SEVARAL AREAS OF RISKS [3] [4], [5] UNDER *(ISO 27002 TO ISO 27005)*

1) CKTECK's Management (Security Policy)

2) CKTECK's Security and Safety Organization

3) Assests Classification and control in CKTECK

4) CKTECK Personnel Safety and Security

5) Physical Safety Security and Environment of CKTECK

6) Incident Management in CKTECK

7) Network security of CKTECK's network infrastructure (WLAN between sites, local area networks)

8) Development and maintenance of systems or Computer and network management in CKTECK(security of premises)

9) CKTECK's Logical access control system

10) Information Technology and Information Security of CKTECK

11) CKTECK's Legal and Compliance matters

12) CKTECK's Application Security and Cryptology

13) Business Continuity and Recovery Planning In CKTECK

4.1.2 INFORMATION SECURITY RISKS AND VULNERABILITIES IN ADVANCED TECHNOLOGIES(Cloud, BYOD and Social Media) OF CKTECK CORPORATION

This section covers the topic of finding advanced information security risks in the corporation CKTECK. As to be considered the latest technologies for CKTECK are CLOUD, BYOD, and Social Media. Therefore in this chapter the author has described the latest, advanced and new information security related risks in these three advanced technologies for the overall areas in Corporation CKTECK.

IN CASE OF CLOUD, OVERALL RISKS AND VULNERABILITIES IN CKTECK CORPORATION

Cloud network computing even have become very popular and beneficial for the organizations but this technology have still some risks and security related issues. Author in [26] says that "*cloud computing gives rise to several data protection implications*". Following are the IT (information technology) related risks in the current cloud network of the modern infrastructure of modern Corporation CKTECK. Threats to Cloud Computing are in several different areas such as related to data locations, segregation, data storage, and data recovery, data integrity, payment, and privacy of sensitive information. Dangerous threat comes from HTTP Denial of Service or XML Based Denial of Service attacks.From the author in [33], "One of the largest disadvantage s of cloud computing revolves around security and confidentiality". These types of attacks are simple and easy to implement by the attacker, but to security experts they are double as difficult to stop. Security vulnerabilities existing in the cloud platform and Security challenges service delivery model are also several threats in cloud. [18]. Following Table11 is related to the several categories and their attributes of cloud risks. Cloud risks are described further in Table12 according to the category related to cloud environment and cloud risks. Author in [8] says that *As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through the adoption of this new model*.

Description of the overall cloud risks in CKTECK, which are listed in the Table12 has been described as following.

C1: Risk of storing personally identifiable information [11]

Because of information can be assessed and operated by cloud provider of CKTECK. Therefore it can be result in misuse of the important and sensitive information of CKTECK in the cloud.

Table11

SR No.	Categories of cloud risks	Attributes and examples
1	Network Security	Encryption, Key management, Secure socket layer
2	Interfaces Security	Authentication, Access control, Protection of client site, identity management,
3	Data security	Backup, Data encryption, Data Isolation and Disaster recovery, Business continuity
4	Virtualization Security	Dedicated hardware, Hypervisor security, Encryption
5	Governance security	Monitoring and management, API's
6	Compliance security	SLA conformity, Standards and certification, Nested Services
7	Legal Issues security	Data storage location and data sanitization

Table 11: Cloud Risks Categorization in CKTECK Corporation, ideas taken from [22] [20] [35]

C2: Risk related to big data storage in cloud is itself a risk [11]

In CKTECK's cloud, a large and big amount of data has been stored. By using social networking sites, users of CKTECK Corporation can leave their logs in the network track. Therefore, it may be result in tracking internal processes and software of CKTECK Corporation by the malicious persons.

C3: Risk of auditing and compliance [11] [21]

In these days there are no all cloud networks which can ensure the integration of the storage access mechanisms. It could be said that there are not confirmed to establish security standards. There could be a risk for CKTECK related to compliance and auditing matters.

C4: Risk of low confidentiality of data [11]

Encryption technique is a security mechanism in the cryptographic theories. But, in the cloud network, the cloud provider has risk regarding accessing the data because the encryption is not strong enough in the cloud. Therefore it is a big risk for CKTECK.

C5: Risk of Low availability of data [11] [21]

There are several reasons for the risk of low availability of data and the information in the cloud network. The cloud network in CKTECK can be compromised by the denial of service attacks.

Table12

Sr. No	CLOUD RISK NAMES
C1	Insecure storage of personal identifiable information
C2	Risk of big and huge data storage
C3	Risk in auditing and compliance
C4	Low confidentiality risk
C5	Risk in availability of data
C6	Insecure SSL risk
C7	Risk of data loss
C8	Risk of data privacy
C9	Risk of data protection
C10	Data leakage risk
C11	Malicious insiders
C12	Risk in data loss when migration of data
C13	Malicious outsiders
C14	Risk of loss of control on data location
C15	Risk of improper security standards
C16	Risk of unawareness by cloud providers
C17	Virtualization and virtual machine risks
C18	Data Sanitization Risks
C19	Risk of difficult backup procedure in cloud
C20	Risk of multi tenancy model of cloud
C21	Risk of service hijacking
C22	Risk of repudiation of information
C23	Risk of insecure API's
C24	Improper key management risks
C25	Data Governance and compliance risks
C26	Risks related to SLA
C27	Improper identity management risk
C28	Compliance and data location risks
C29	Privileged user access risks
C30	Risk in investigation support and forensic investigation
C31	Risk of natural disasters
C32	Risk of unavailability of cloud network
C33	Risk of difficulty in recovery in failures from disasters serious incidents
C34	Risky mitigation procedure in case of business continuity

Table 12: Overall Cloud risks in CKTECK Corporation according to categorization, ideas from [18] [20] [22] [35] [11] [21] [13] [14] [15] [35]

Denial of service attacks can hijack [13] the servers of CKTECK. Therefore the attacker can stop the web services of CKTECK from the functioning of operations.

C6: Risk in Secure socket layer [13]

Secure socket layer in the CKTECK's cloud can be vulnerable due to the man in the middle attack. Hence it can fail the authentication schemes if it is incorrectly configured by CKTECK's employees.

C7: Risk of data loss, phishing, botnets [13]

There may be possibility in the CKTECK's cloud environment i.e. vulnerable to the phishing and bots. These are the serious problems in the cloud network which may results in the loss of CKTECK's data and the software.

C8: Risk of data privacy [13][77]

Risk of data privacy is one of the biggest security issues in the cloud network of CKTECK. The regulations of the personal information can vary across the world due to several subsidiaries of CKTECK at different locations in different countries. Data and information of CKTECK are not remains private because it is also even stored outside the country.

C9: Risk of data protection [13]

Tt is very difficult for the consumer of cloud to effectively check the data is handled in a lawful way or not? Hence it is very risky for CKTECK.

C10: Risk of data leakage [13] [14]

There is no proper control on the data which is stored in the cloud. It can be leaked to the malicious persons by new hacking techniques or by malicious insider persons in CKTECK.

C11: Risk of insider threats and malicious insiders [15] [22]

Malicious insiders in the CKTECK can harm the reputation and financial status of it. Insider threats are that threats which arise within the organization. Some reasons are lack of transparency, processes to hire new employees, keeping data at different locations, relations to the third parties, casual hackers, adversary with the view of corporate espionage, are some examples of the insider threats. Insider threats are always present within the organization. According to IDC (International Data Corporation) survey findings, 440 organizations have found by insider threats. Some other more examples of insider threats are rouge cloud provider, rouge administrator, unauthorized attempt of organization employees, exploitation in cloud weaknesses by insiders etc. It could be a big risk for CKTECK.

C12: Risk of lost of data through migration of data [15]

Due to the migration of data in CKTECK's cloud, the level of the data can be compromised. It is because the cloud has multilevel environment. Hence, it is very difficult to maintain the access control, authentication etc. in the cloud. In clouds there is also very difficult to maintain the same level of data.It could be risky for CKTECK in data loss, financial status loss, reputation loss, customer count loss and so on.

C13: Risk of malicious outside attacks [15]

These are most concerning issues regarding the security in the cloud. Some of the examples are hackers, attackers, tapping, breaking by social engineering etc. It could be harmful for entire CKTECK.

C14: Risk regarding loss of control on data location [15]

The services and data of CKTECK which are ported into the cloud is without awaring its location. Therefore the data and the services location can be anywhere. Hence the CKTECK can lost its control on it. It is because the data is located on the unknown place. So it is very difficult for the Corporation's employees to control this issue.

C15: Risk of no standard security specifications and loss of control [18] [21]

Cloud environment has no proper security standards and specifications. Therefore it is very difficult to maintain the CKTECK's cloud security. Moreover in the cloud there is no proper control on the security controls which are implemented on the user end.

C16: Risk of unawareness by cloud providers to hosted services [18]

Due to this risk, it is very difficult for cloud providers to produce secure effective and efficient security controls. Hence it is risky for CKTECK.

C17: Risk of virtual machines and virtualization [18] [22]

The reasons for risky virtual machines environment are malwares and advanced viruses. Virtual Machines are also risky when these machines are offline too. Moreover virtual files can be compromised by injecting malicious codes. Furthermore the template used VM can retain the information of the original owner, which can be used by new consumers. Moreover VM's are insecure. Several VM's are running under a VM monitor in the cloud network. In this whole CKTECK network, multiple servers are attached with the one host. Therefore, it could be result in no separation between CKTECK servers. Hence this is vulnerable for threats like malicious attacks.

C18: Risk of data sanitization [20]

It is a serious risk in the CKTECK cloud infrastructure. In simple words can we imagine that what will happen when the cloud service is terminated? Moreover what will happen to the data of the user of CKTECK?

C19: Risk of difficult backup procedure [20]

The backup procedure in any cloud network is very important so that the lost data could be restored. The backup procedure in CKTECK's cloud environment could be difficult because of data storage at unknown locations.

C20: Risk of multi tenancy property of cloud [21] [22]

Cloud works on multi tenancy model which means that cloud services are scalable in the shared infrastructure. Hence is not strongly isolated. Moreover security must be considered in all aspects like confidentiality, availability, integration etc. It is also risky for CKTECK.

C21: Service Hijacking risk [21]

By this, the attackers can gain access to the services of CKTECK.It is because the cloud is not strongly secured. Services for instance E Commerce, E Transactions, E mail etc. can be exploited. Furthermore an attacker can gain illegal access to the cloud network and the customer's login. Hence, attacker can regain the sessions of transactions by sniffing, phishing, eavesdropping, replying the information.

C22: Risk of repudiation of the information [21]

Sometimes cloud provider can't claim that the information transmitted was correct or not. It is a risk of repudiation of the information in the CKTECK cloud network.

C23: Risk of insecure API's in cloud [22]

The main role of API is provisioning, monitoring and management of the processes which are running in the CKTECK's cloud network. API's are designed to provide protection against accidental as well as malicious attacks. The main features of API's are encryption and monitoring of the activities. Attackers are also very smart in these days. They can use several methods for finding keys. Even cloud services are also shared with third parties. Therefore these are vulnerable for improper implementation by CKTECK employees, using weak encryption schemes, shared third parties etc.

C24: Risk of improper key management in backup [22]

If the keys are not properly managed and implemented by CKTECK employees then it may result in compromise all encrypted data. Moreover it provides a great difficulty in maintaining the backup procedures for the CKTECK employees.

C25: Risk related to Data Governance and Compliance [22]

Third party provides a main role in the cloud. If there are no proper terms and conditions under an agreement then there is always a risk of data leakage and misuse of data. Hence information security governance should be proper.

C26: Risk in SLA [22]

SLA is service level agreements. It is an agreement which describes the performance criteria related to the service and the client. There is always a risk for CKTECK because of lack of trusts in the clients and loss of data governance. It may be result in no guarantee in CKTECK regarding the effectiveness of security and privacy controls.

C27: Risk of Improper Identity management [22]

Identity management is the base of CIA, which is the base of information security. If is not managed properly with granted access then it may harm the CKTECK cloud network.

C28: Risk of compliance and data location [35]

There is always a risk in CKTECK's cloud regarding this. Data location is a big issue in the cloud computing related to the privacy regulations in different jurisdictions.

C29: Risk of privileged user access [35]

It could result in risk of malicious insiders, risk of account and credential hijacking, risk of data manipulation and risk of damaging reputation and financial status of whole CKTECK Corporation.

C30: Risk in investigation support and forensic investigation [35]

In cloud, there is no or little visibility on the deleted media. Therefore low backup and recovery procedures are there. Moreover there is always a risk for CKTECK employees of difficulty in the forensic investigation too because of data at several unknown locations.

C31: Risk of hardware & software failure due to natural disasters [22]

Risk of natural disaster can't be avoided by anyone. This can be result in huge loss of computer hardware and software.

C32: Risk in unavailability of cloud network [35]

There could be chances of the risk of unavailability of services in the CKTECK's cloud network. For instance (1) Salesforce.com was unavailable on 6th February 2008 which was followed by S3 and EC2 cloud, (2) Amazon S3 was unavailable again for eight hours in same year 2008 and (3) There was a multiday failure of Amazon EC2 in April 2011.

C33: Risk in recovery from disasters [35]

In case of no prior planings of disaster recovery and backup procedures by CKTECK employees then the recovery from disasters is very difficult and impossible for CKTECK's employees.

C34: Risk in mitigation of cloud service in case of business continuity [35]

Improper performance checking, improper profitability, improper local storage capacity, irregular backups and data on local services, improper contingency plans are some threats of clouds in the business continuity. It could be risky in the mitigation of cloud services in CKTECK in case of business continuity.

IN CASE OF BYOD, RISKS AND VULNERABILITIES IN CKTECK CORPORATION

Employees of CKTECK feel very flexible while using their own devices on their jobs too. BYOD has been taken its place of an emergent era in modern CKTECK. Higher Authorities of CKTECK are attracted in BYOD because of flexible features of these technologies for instance user friendly nature, light weight and easy to carry, more compatibility for users by using their own devices at job, connecting with social networking sites on own device is more flexible in nature, flexibility of doing job related tasks in homes on own devices and many more. Even though the BYOD has made the life of a normal employee of CKTECK very flexible and easy, but on the other side it has increased the chances of more security related risks to the CKTECK Corporation and problems to the organizations too. Author from [71], present his views that BYOD have shown a part of emerging Information Technology models that are related to portable devices and mobility. Using BYOD has become a huge attraction for the upcoming employees because they can also do job related tasks at homes and personal tasks at jobs etc. From Cisco's point of view employees are

also willing to pay money. Even more Cisco's employees are paying 600 dollars averagely to use BYOD [71]. Moreover BYOD is a business policy which allows and encourages the employees to bring personal devices at workplace and use them to access organization's resources for instance emails, intranet, applications of organization and so on [74]. Table 13 shows BYOD Risks categories for CKTECK and Table 14 shows overall BYOD Risk names in CKTECK. The description of overall BYOD risks for CKTECK Corporation shows after Tables13 and 14.

Table13

SR No	Categories of BYOD Risks
1	Risks related to device attacks
2	Risks related to advanced malwares
3	Risk related to physical access
4	Risks related to Insider Threats
5	Risks related to communication
6	Risks related to compliance

Table 13: BYOD Risks Categorization in CKTECK Corporation, ideas from [71] [74] [75] [81] [85] [86]

B1: Risk of device lost or stolen [71]

There is always a risk for CKTECK organization in BYOD, when the device is lost or stolen by any malicious person. With this the risk is related to misuse the CKTECK's secret information and sensitive personal information of the owner of the device too. With bad ideas in mind like reputation and financial loss of enterprise CKTECK, any bad person can illegally use the identity of the device owner. It is because in the devices there are stored personal accounts, personal chats, and emails of CKTECK's employees in common inbox of all combined accounts. Therefore bad person can take misuse of it. This is really a big risk in modern CKTECK while using BYOD.

B2: Risk of attacks from the devices [71]

Employees in CKTECK are great fans of the internet. Internet with advanced technologies plays a great role in everyday's life. The personal devices of employees at CKTECK are almost attached with internet. Furthermore the nature of the internet is insecure. There is always a risk of device attacks while using internet. Hence, the security of the devices can be compromised because of this. This is risky for the CKTECK.

B3: Risk of data Loss [71] [85]

Data loss refers to when the unauthorized movement of the data which occurs outside the control environment of the CKTECK network. It may be result in data loss.

Table14

Sr. No	BYOD RISK NAMES
B1	Risk of lost or stolen device
B2	Risk from device attacks
B3	Risk of data loss
B4	Risk of data tampering
B5	Risk of data unavailability
B6	Risk of unmanaged and untrusted devices on corporate network
B7	Risk of malware migration
B8	Risk of no control on personal devices
B9	Risk of disclosure of private and personal data due to togetherness of storage of personal and corporation data
B10	Risk of no protection of network device
B11	Risk of no device protection
B12	Risk of uncontrolled device and enforcing compliance
B13	Risk of unknown IP Address
B14	Risk of advanced threats
B15	Risk of insider threats
B16	Risk of advanced mobile designed malware
B17	Risk of exploiting vulnerabilities in mobile systems
B18	Risk of no proper security standards for mobile devices
B19	Risk of no visibility to the end users
B20	Risk of insecure antivirus
B21	Risk of no control on users downloads
B22	Risk of data extraction can be done easily by intruders
B23	Risk of new culture of hacking techniques
B24	Risk of industrialized attacks
B25	Risk of employee Misuse and abuse
B26	Risk of fully automated attacks
B27	Risk of mobile threats

Table 14: Overall Risks Scenario in CKTECK in BYOD

B4: Risk of data tampering [71]

Unauthorized modification of data can be counted as data tampering. Any malicious person can do modifications in data as a purpose of killing the good reputation or finance loss for the organization CKTECK. It could be result in big loss to the enterprise because of lost of correctness of the original data.

B5: Risk of data unavailability [71]

There could be a risk of unavailability of data in using BYOD. It could be the result of denial of service attacks [11] [21] or other hacking attacks on the devices of CKTECK'S professionals.

B6: Risk of unmanaged and untrusted devices on CKTECK network [74]

The mobile devices sometimes not under a full control of the enterprise. When these are not controlled and managed and secured by the security mechanisms in the enterprise CKTECK then there is a chance of risk of misuse and destroy of the information of CKTECK organization.

B7: Risk of Malware Migration [75]

When personal devices are attached to the corporate CKTECK's network by Wi Fi or any wired network then there may be risk of migrating malwares from the devices to the whole network of CKTECK and its machines too.

B8: Risk of no control on data on personal devices [75]

When the CKTECK's information migrates to the personal devices then after that there is no control on that information from the organization side for instance CKTECK's data becomes no longer under control. Therefore in this situation data and other related necessary things are under risk of misused illegally or destroyed or modification and so on.

B9: Risk of disclosure of private and personal data due to togetherness of storage of personal and corporation data [75]

When the personal and corporatio's l data of CKTECK's employees is stored on same device then it would be very difficult for CKTECK to maintain security. For the organization CKTECK it is very difficult to implement the barriers when personal and corporate data is stored together in same device. In this case there is always a risk of disclosure and visibility of CKTECK's information by employees of CKTECK to others.

B10: Risk of no-protection of network traffic [80]

If the devices at CKTECK are without some protection mechanisms in proper place which can secure network traffic then there is always risk to the corporate information. Information could be lost or could be hijacked by malicious hackers. Even it could be misused in monetary terms or any other usage.

B11: Risk of no device protection [80]

This risk comes into place when the CKTECK's employee as the owner of the device is not using it directly or he/she have not any direct management to the device who can say that the device is protected properly or not from other persons? Hence this is a big risk for CKTECK.

B12: Risk of uncontrolled device and enforcing compliance [80]

By using BYOD at CKTECK, there is always a risk that how to enforcing compliances properly with the guidelines of the corporate when employee is on the move.

B13: Risk of Unknown IP address [80]

In case while using BYOD, It is a possibility when The employees in CKTECK don't know that who is using a particular IP address and the identity isn't being used as a element of the policy.

B14: Risk of advanced threats [81]

Due to the enhancement of new technologies, the new security related threats have been emerged too for instance key loggers, malwares, cyber attacks, bot nets etc. These threats may results in creating risk of unauthorized access and the information of organization CKTECK. Furthermore it can be stolen from the endpoints. Moreover there also some bad effects of this like data leakage risk and malware distribution risk.

B15: Risk of Insider threats [81]

Insider threats have been growing from the few recent years. The insider threat is a risk which is always present in the organization. For instance a malicious employee in CKTECK can steal corporation secrets, intellectual property, and sensitive customer's information. Rouge and clever employees at CKTECK can steal corporation's data by saving it locally through drop box's accounts. They can forward organizational secret email by using personals accounts. Hence malicious person inside the company can misuse the data and this may again result in reputation and financial loss. From [81], according to Verizon, 48 percent of employees were insiders who did malicious activities and data breach in 2009. Third party persons, persons from trusted parties, can also come under this category. Insiders have easy way to tap the corporation information because they are known of security gaps within the organizations.

B16: Risk of advanced mobile designed malware [81]

When employees at CKTECK install the applications on the personal devices including games, music, media, social networking and so on then there is always a risk of viruses, bots and other mobile designed advanced malwares. When the employees at the job place access the corporate network then there is always possibility of leaking information of CKTECK to malicious outsider because these devices are unmanaged and the employee may be careless in this case. It can be done simply by saving the file which is opened from webmail or sharepoint to their local file system. With this information easily can be stolen by malware applications.

B17: Risk of exploiting vulnerabilities in mobile systems [81]

This is a main security concern and a risk to the corporation CKTECK in following the BYOD. When the employees of CKTECK have no control in place for the usage of the mobile devices and when the employees are ignoring existing security policies then the vulnerabilities of the devices can be exploited easily by the hackers or false persons.

B:18 Risk of no proper security standards for mobile devices [81]

Security standards like authentication, SSL encryption, IPS, firewalls etc are not always secure against advanced malwares and there the perfectly secure mobile security standards have not

been discovered. From [81], found that there was a security breaches in certificates authority. Recently, a malware has been stolen data, noted keystrokes and recorded conversations by using a hash collision. Even SSL is also insecure because it uses random numbers for generating certification. And it is very easy to compromise the security of information. This leads a high risk to the enterprise CKTECK.

B19: Risk of no visibility to the end users [81]

In these days in BYOD there is always a risk of no visibility of the data into the end users. There is not security and surety regarding under this phenomena.

B20: Risk of insecure antivirus [81]

Anti viruses are used to save from the viruses. Even in today's modern infrastructure of technologies the anti viruses are not fully effective from advanced malwares. For instance man in the browses attack (MitB) sits in web browser between the user and the website. It can alter and change the data. Similar threat man in the middle is also related to this. It is so dangerous and can used for stealing online banking information. For instance some can steal user logins and passwords credentials. Additionally it is putting web based corporate data on the risk.It is risky for CKTECK too.

B21: Risk of no control on users downloads [81]

In case of using personal devices on the workplace area at CKTECK, the corporate itself is unable to control several downloads by the users. For example IT Professionals and Administrators at CKTECK have no control that which browser is being downloaded and used by the employees of CKTECK. Surprisingly nobody can know which security patches and plug-in have been installed and used by the employees of CKTECK. This can lead high risk for Corporation CKTECK.

B:22 Risk of data extraction can be done easily by intruders [81]

It is very difficult to check and see in the user devices at CTECK that is it with which viruses? The CKTECK Corporation's administrators and other higher responsible persons are even unable to see or manage the stored information, cache, cookies, password storage, browser history etc. Data in the devices is remained in cleared text format which can be extracted easily by the intruders and advanced malwares. Moreover the cut, copy, paste, and deleted data is remained in clear text form. Hence it can be misused by smart hackers.

B23: Risk of new culture of hacking techniques [86]

Hackers and intruders are also smart and advanced in these days. These malicious persons can gain success very smartly and easily in finding of secret information of CKTECK. They can exploit vulnerabilities in the Corporation CKTECK system. There are some advanced hacking techniques has been developed. From [86], the face book in mobile users has increased the chances of exploitation by hackers. Every time online on these devices may result in migration of new spams which results in denial of service attacks, data theft risk etc. It also has risk of data breach because personal information is shared on personal devices with the attachment of internet. Another related example from [86], From Verizon data breach Investigation reports, there was 100 million of records were stolen by hackers via data breach in the year 2011. This kind of risk is very high for the organizations and for CKTECK too.

B24: Risk of industrialized attacks [86]

Industrialized attacks are related to the world of cyber attacks. Recent related example is SpyEye banking malware. Cyber criminals are involved for making such kind of bots. By this the attackers were able to manage a group of botnets for the purpose of spamming, key logging, in order to get credit card and personal information. Even large or small, both type of organizations may have risk under this.CKTECK is also under this risk.

B25: Risk of employee Misuse and abuse [86]

This is a high risk and big problem for CKTECK enterprise. Furthermore employees of CKTECK can cheat and misuse the organizations information by restricting the policies. With BYOD, there is difficult process for administrators at CKTECK to secure properly the new devices which is entering into corporation systems.

B:26 Risk of fully automated attacks [86]

Automated attacks are the attacks which are designed by the hackers for the automatic migration of malwares into the system. These attacks come into action when the author of the device is busy with the other jobs and he/she is not using device directly. Related example is SQL shammer, which compromised the servers on the internet automatically.These are risky for CKTECK also because employees at CKTECK may be attacked by such kind of attacks.

B27: Risk of mobile threats [40]

Mobile threats are like mobile worms on victims, malicious mobile applications, mobile malwares, Sms spams, smishing and vishing [37](Smishing is a kind of phishing attack which uses text messages on phone for attack and vishing is the confidential information is solicited over the phone) etc. It could harm the CKTECK's employees and information too.

IN CASE OF SOCIAL MEDIA, OVERALL RISKS AND VULNERABILITIES IN CKTECK CORPORATION

From [50] author describes that "Social networking sites offer interesting features to attract people to use them; yet it is a notable fact that social networking sites security, access controls and privacy are weak by design" . Even in [65] author explains that social media have really changed the way people built their online personal work. But if the employees will use social networking with carelessness then it could be result in data loss, reputation loss, financial loss and many more. Along with the positive side social networking media and sites have negative aspects. Even though this media have interesting features like easy way of messaging, getting answers quickly from the online friends, instant messaging, quick file sharing, video conferencing and so on. Employees at CKTECK are allowed to use of social media so that they can take the advantages of this modern technology. Even social media have changed the life and working style of CKTECK's employees. Author in [10] explains that

> "Web 2.0 and social networking sites offers fantastic opportunities for the organization and individuals, but they come with risks and it will take us sometimes to fully understand them and manage them"

. Employees feel comfortable and easy by using these social media benefits. But in recent study these sites have raised the chances of security and privacy concerns for the users. Risks in social

media networking at CKTECK could be related to privacy, security, trust [65] and web related. Social media risks for CKTECK can be categorized as follows in Table15 . The overall risks under these categorization are presented in Table16 . Moreover the description for these risks has been described.

Table15

SR No	Categories of Social media networking Risks
1	Risks related to privacy issues
2	Risks related to security issues
3	Risk related to trust issues
4	Risks related to web threats issues

Table 15: Risk categorization in Social Media at CKTECK, ideas from [41],[43],[46],[47],[48],[49], [50],[53],[55],[56],[58],[59],[61],[62],[63],[65],[67]

SN1: Risk of disclosure of private information on the sites [48]

Popular social networking sites like face book and myspace can contain personal information of a person like gender, birthday, relationship status, job place, employment history, education history etc. This information can be misused by the malicious persons and they can also send fake information to the CKTECK organization where the employee is working. Therefore there is a risk to CKTECK Corporation of data and services to be compromised further.

SN2: Risk of malicious third party [48]

While using the social networking media at CKTECK's workplace, there is sitting third partied behind this services which are seeking the information of the users of CKTECK. While using CKTECK organizational network the employees can leave the signs of the valuable information and data to the third parties. There might be the chances of misuse of the CKTECK's information if the third party contains malicious persons and intruders. Malicious 3rd party application might run with social networking sites. With this, they can achieve secret data and can get access to other applications in the organizations. Hijacking profiles can be done also by this.

SN3: Risk of unauthorized access to data by hackers [49]

By the use of social networking sites by CKTECK employees, hackers can get chance to easily gain unauthorized attempt and access to the private and confidential data of corporation CKTECK. They can find vulnerabilities in the CKTECK's system by entering from their sites and CKTECK's data might be misused in illegal way.

]

Table16

Sr. No	SOCIAL MEDIA RISK NAMES
SN1	Risk of disclosure of private information on the sites
SN2	Risk of malicious third party
SN3	Risk of unauthorized access to data by hackers
SN4	Risk of gaining access to the secret information of organization
SN5	Risk of getting private conversations of the organization
SN6	Risk of social phishing
SN7	Risk of inability to control the information regarding user posts in Social Networking
SN8	Risk of online identity theft and identity misuse
SN9	Risk of online scams, viruses, malwares, network intrusions and spyware
SN10	Risk of location tracking from mobile social networking
SN11	Data manipulation risk
SN12	Risk of data retrieving
SN13	Cybercrime risks and cyber threats
SN14	Risk of data misuse and abuse
SN15	Risk of social engineering attacks
SN16	Risk of fake antivirus
SN17	Miscellaneous Risks

Table 16: Overall Risks In case of Social Media networking at CKTECK

SN4: Risk of gaining access to the secret information of organization CKTECK [49]

This kind of risk comes into place when anyone wants to security breach. By watching a username and password one can gain access to the confidential data of employee and organization. Malicious insiders can take advantage of this. It might be happen with CKTECK's employees also.

SN5: Risk of getting private conversations of the CKTECK [49]

This risk occurs when employees at CKTSCK are instant messaging related to personal and private issues of organization CKTECK on the social networking sites. This can be leaked to the malicious insider, which can get username and password. Later he can misuse it.

SN6: Risk of social phishing [50]

While using social media at CKTECK there may be chances in a risk from phiser's side. He can look at any one of the growing number of services to CKTECK's employees information and about relationships. Because of circle of friends on social networking sites, a phiser can harvest large amount of reliable information. It is because the terms of service of these sites may disallow the user from allowing spam, phishing, other unethical and logical activities etc.

SN7: Risk of inability to control the information regarding user posts in Social Networking [50]

While using social media and networking, employees at CKTECK are in touch of posting messages and status on these sites. If they are posting some information related to the CKTECK personal information, then it may be misused by malicious persons.

SN8: Risk of online identity theft and identity misuse [50] [56] [59] [60] [64]

Online identity can be comprised with advanced methods. By the use of social networking sites it is possible for intruders to steal the important details regarding user identity and related credentials. Therefore results may be highly dangerous for instance money theft from digital accounts, identity misuse in cybercrimes and so on. It could result in money and reputational loss to the CKTECK.

SN9: Risk of online scams, viruses, malwares, network intrusions and spywares [50] [53] [64]

Social networking sites are victim of insecure transfers. There may be presence of viruses, worms, spywares and online scams in these sites. It could be result in stop functioning of several applications of the organization CKTEK. It can also corrupt the important files and documents of CKTECK and so on. For instance orkut was hit by worms which were attempted to steal banking information by checking a link JPEG. Moreover orkut users were been targets of twitter based scams. This URL which was embedded in tweet can make user agree to download a fake flash update and so on. Later it can harvest Google account for exploit at other harmful activities. Furthermore social networking scams can exploit the height ended levels of trust that tend to exists for the communication on the site.

SN10: Risk of location tracking from mobile social networking [53]

Smart phones are recent trend of CKTECK corporation. Smart phones have applications related to location based services. Location tracking services can identify user's location in several ways. It is related to privacy issues for instance social security number, full name and address and other associated details could be compromised by using these location based services.

SN11: Risk of data manipulation [54] [69]

According to SANS institute in [69] *"An attacker could deliberately modify data in transit or storage through malware or direct manipulation, but legitimate users also make honest mistakes. Unintentional misinformation is frequently posted on the Internet, which is then taken as fact by many viewers. In social media, data is stored in many places where many different users can access it. Having data accessible to many users increases the chance that a malicious or mistaken user could post inaccurate information, which compromises data integrity"* For CKTECK employees this kind

of risk is also very harmful.

SN12: Data retrieving risk [54]

Malicious persons can retrieve the CKTECK's data by using social networking sites. The aim of malicious person is might be to suspect the machines and systems of CKTECK.

SN13: Cybercrime risks and cyber threats [54] [63] [61] [63] [64]

Social networking websites are vulnerable in cybercrimes, phisers, fraudsters, child predators and so on. Cyber threats had been emerged with the emergence of these sites. The aim of cyber threats might be very dangerous like failure of CKTEK's network servers, failure of CKTECK's routers, stop functioning of enterprise machines, failure of overall network of CKTECK and so on. Hence it might be very dangerous.

SN14: Risk of data misuse and abuse [54]

By using social networking sites there is always risk for CKTECK for the misuse and abuse of data.

SN15: Risk of social engineering attacks on CKTECK's secret data [60] [63]

There are several social engineering attacks which can exploit and destroyed the reputation of organization by misusing the organizational information. Social engineering attacks are very common these days like spreading harmful Trojans, malicious malwares, sexual grooming etc.

SN16: Risk of fake antivirus [64]

This type of risk uses social engineering to make fool to the victim employees of CKTECK by loading the malware. Fake antivirus takes file hostage and then encrypts them and requires the employees to wire the money. It may be result in big money loss to the Corporation CKTECK.

SN17: Other miscellaneous risks [62]

Some other several risks of social networking sites to the CKTECK are: Risk of diminished CKTECK's employee productivity, Risk of diminished IT bandwidth of CKTEK's resources and services, Risk of loss of confidential data of CKTECK, Risk of violation of confidentiality policy of CKTECK etc.

4.2 TASK 2 SOLUTIONS, i.e TO DEFINE SECURITY POLICY

This section is about solutions to the tasks which are already given in Task 2nd i.e. To Define Security Policy in Subsection 3.8.2.The subtask 3. is "As, considering yourself a CISO in CKTECK how will you be able to maintain the security policy management? How can you create, issue and maintain CKTECK's information security policies, standards, guidelines, processes and procedures?"

The following description and explanation is the solution for this. This solution is an example solution as a training material for the students. The ideas for finding solution have been taken from [90]

4.2.1 PURPOSE AND GOAL FOR MAINTAING SECURITY POLICY MANAGEMENT AT CKTECK

The main goal of policy management schemes in CKTECK is to refer the practices and methods which are used to create and maintain CKTECK's security policies to translate, clarify, and communicate with CKTECK's management's position on high-level security principles.

4.2.2 OBJECTIVES FOR MAINTAIN SECURITY POLICY MANAGEMENT AT CKTECK

The some of the objectives for maintain security policy management at CKTECK Corporation is listed below.

- To provide CKTECK's management direction and support for information security in accordance with business requirements, relevant laws and regulations, and state policy.
- For creation, issue, and maintaining the security policies, standards, guidelines, processes, and procedures at CKTECK

4.2.3 ROLES AND RESPONSIBILITIES OF CISO IN SECURITY POLICY MANAGEMENT AT CKTECK

Chief Information Security Officer at CKTECK has several roles and responsibilities. Following list is related to sub areas which comes under Security Policy Management

1. Executive Communication (It means to provide management advice and recommendations for the CKTECK's information security management program)
2. Policy Development (To develop and maintain security policies, standards, guidelines, processes, and procedures of CKTECK)
3. Policy Compliance (To oversee the monitoring and compliance with policies, standards, guidelines, processes, and procedures at CKTECK)
4. Employee Acknowledgements (To create a security policy acknowledgement process for CKTECK)

The several roles of CISO of CKTECK in these sub areas related to Security Policy Management at CKTECK, has been listed below.

Executive Communication

- CISO should be responsible for coordinating a governance structure. He should be responsible for developing, reviewing, approving new or revised policies, standards, guidelines, processes, and procedures of CKTECK Corporation
- CISO should be responsible for providing updates on existing or pending laws, regulations, or statewide policies, security issues or incidents, and the potential impact to the CKTECK Corporation.

Policy Development

- CISO should develop and document a formal process for creating, updating, and adopting CKTECK's security policies. He can do reviews by the CKTECK's Legal Officer, Human Resources Officer or any other key stakeholders.
- CISO should create a governance committee and develop a charter, identify roles and responsibilities, and set goals and objectives.
- CISO should schedule regular meetings with the committee to discuss security policy, standards, guidelines, processes, procedures, and issues.

Policy Compliance

- CISO should responsible for review existing internal controls in place to monitor and report exceptions or violations and prepare reports of findings.
- He should recommend improvements for CKTECK's better compliance.
- He should provide executive management and the committee with status reports and updates regarding compliance.
- He should be responsible to review and report how incidents or threats (such as unauthorized access, misuse, modification, duplication, or disclosure of information) are handled and controlled for compliance.

Employee Acknowledgements

- The CISO should be responsible for oversee the CKTECK's compliance with information security acknowledgement processes.

- The CISO should ensure the process includes the use of acceptable use banners and an employee acknowledgement form in CKTECK related to compliance.

5 ADVANCED AND HOT ISSUES IN THE FIELD OF INFORMATION SECURITY

Information Security can be defined from [38], NIST as, *"The protection of systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability"* Moreover from [39], information security is related to confidentiality, integrity, availability, authenticity, accountability, non repudiation and reliability of the information. Information Security has become important need and issue in all type of modern organizations in now these days because everything is going to be modern and advanced. Networked and modern society has increased more chances of internet related problems which destroy the confidential and important information in the organizations. Several security related threats and risks have resulted in several security breaches. Following information is related to current and hot issues in the area of information security in recent years in several enterprises. In following information there will be real examples and proofs of several security breaches in recent years in several countries.

5.1 SURVEY BY PWC CORPORATION, SECURITY BREACHES SUYRVEY 2013 IN LONDON [39]

The overall report of this survey shows several findings for instance (1) Due to unauthorized attempts the security was breached of 78 % large size and 63% small size organizations (2) Denial of service attacks breached security of 39% large size and 23% small size organizations (3) By penetration from hackers breached security of 20% large size and 15 % small size organizations (4) 14% of large size and 9 % of small size organizations lost their intellectual property and confidential data by outsiders attacks (5) Average cost of worst security breach in large size organizations was 450 K to 850 K and in small size organizations was 35 K to 65 K billions of pounds per anum. By reading the survey several real examples of security breaches have found in London. The security breaches were in small, medium and large size enterprises. According to the survey several true examples are shown in Table17 and Table18 below.

5.2 SURVEY BY WEBSENSES CORPORATION, SECURITY THREAT REPORT 2013 [63]

The overall findings of the survey report shows that almost 600% of malicious web links have been increased worldwide in last year. 32 % of malicious links were used by social networking. 82% of malicious links were sent by sms. In case of emails, only one from five emails was sent safely and the rest four were unsafely sent. The compromised legitimate websites were from

Table17

PWC, Information Security Breaches in London, 2012

SRNo	Organization	Security Breach	Reason Of security Breach	Results
1	A large technology enterprise	Website of the enterprise was accessed by hackers	By using a known vulnerability in the system	Enterprise suffered significant adverse media coverage after taking a month to restore business
2	A small insurer enterprise	A huge amount of data security was breached by web crawlers and made it available in search rankings	Enterprise didn't focus on security and security provider	Took a month in discovering the problem and the systems were offline for a week to fix this problem
3	A small telecom provider	Total data loss	Employee with infected laptop	Enterprise had to provide extra training to other employees for dealing with security risks
4	A large manufacturing company	Confidential data was misused	Malicious and rogue insiders	It took several man weeks and resulted in reputational damage by media coverage
5	A large pharmaceutical company	Internal network of company was accessed by an attacker	Because of poorly configured technical configuration and not up to date	Took 100 man days, and cost of 100,000 pounds .Company deployed new security systems and changed its policies and procedures
6	A medium size energy enterprise	Disk of storage area network was corrupted	Because of insufficient redundancy on it	It took a month to recover and several man weeks effort and tens of thousands of pounds were spent on it
7	A government organization in south west of London	Breach of private and sensitive data	Because third party released sensitive and private data accidently	Loss of business, several man week efforts tens of thousands of cost. They took legal actions against responsible persons and increased security in third party
8	A large insurer	Breach of files with	A contractor	A big financial loss

Table 17: Hot issues in information security in enterprises in London, 2012

Table18

	company	sensitive information	downloaded it illegally by using removable media on his termination	more than 10,000 pounds
9	A small Yorkshire charity	Computers were infected	By clicking on link and it spread viruses	No big loss, it was removed with antivirus
10	A large bank in Central London	Failure in main payment system	Because system change in bank went wrongly	Erroneous payments were made by bank
11	Medium size technology company	Important data was been deleted by employee	Due to lack of awareness and poorly designed configuration	It took a month for restore the system and several man weeks efforts.
12	Large technology company	Data was leaked and lost from stolen laptop	Laptop was stolen from parked vehicle due to lack of physical security	Financial loss and several man weeks efforts to recover data
13	Small security consultancy firm	Emails were sent to all recipients with inappropriate response by employee	Employees mistake and unawareness	Loss of money, business and Customer's complaints.
14	Medium size government enterprise	Public websites were harvested by employee	Misuse of security training by employee	Reputation damage and consumption of several man weeks of management time
15	Government enterprise in channel islands	Big data loss	Due to Hard disk failure and third party replaced it with virus infected hard disk	Results in serious business disruption and man weeks effort to recover
16	Large insurer enterprise	Data loss	Because of poor backup processes	Financial loss in recovery process
17	A large insurer company	Failure of monitoring alert systems	Ineffective contingency plans	Big financial and business loss. Recovered after long time
18	A large technology company	Private Information leaked	Because it was discussed by employees	Reputational damage and provided extra additional security training to employees
19	A large technology company	Business disruption for long time	Because of catastrophic power outage due to insufficient testing of generator switch-over processes	Took several man weeks and money loss
20	Medium size technology company	Primary servers were failed	Because of super storm sandy	Took 24 hours to recover and client facing systems were being unavailable

Table 18: Hot issues in information security in enterprises in London, 2012

area of Information technology, Business and economy, Sex, Travel, Shopping etc. Moreover all malicious websites were from Information technology, Search engines and portals, News and media, Social networking, Advertisements etc. Some of the key findings, related to the field of information security hot issues, by web senses security threat report 2013, have been shown in Table19

Table19

Web senses Information Security Breaches worldwide, 2012

SRNo	Categories of recent emerged threats	Threat Examples	Explanation
1	Web related Threats	For instance legitimate sites serving internet, malware hosting, Web threat victims, malicious web blogs	Web threats were very malicious in 2012. According to web senses, there was 6-fold increase in malicious sites overall. Furthermore 85 % of malicious sites were found on legitimate web hosts which had been compromised
2	Social risks	Malicious web links, Malicious applications on face book and twitter, Social malwares, *"Pak Hack attack on face book", "Christmas Themed face book scams"*	Face book was found with suspicious contents and postings during the analysis. Twitter was found in spreading malicious links and threats. More than 500 billion users were found of twitter. USA is the country which is on the highest rank in number of use of face book.
3	Mobile Threats	Lost devices, Malicious mobile applications, Social risks like internet browsing, gaming, social networking, dangerous location based services, malicious notifications, android *"gold dream"* malware, malicious emails, malicious mms	Web senses found that 82 percent of malicious applications s an SMS messages as a part of their attack. Moreover the it found that one in the ten malicious applications asked for permission to install other applications. 73.6 % of mobile phone users were actively connected to the face book. According to report the total numbers of mobile face book users were 680 billion.
4	Email Threats	Like Spams, Phishing, Malicious URLs, Fake URLs, Infected sites and so on	Research found that last year there was emergence of multistage attacks in the emails. These attacks contributed Malware infections and data theft. Web senses found that only 1 in the 5 emails were sent legitimate. Research concluded it could be very dangerous for network infrastructure of the organizations. Moreover mobile phone users are also increasing. This is really very risky. Emails were found victim of phishing, scams, spams etc. In phishing USA is again on the top highest.
5	Data Theft/Loss Threats	Stolen personal identifiable information, Stolen intellectual property, Insider threats, credit card breaches	Data theft and lost attacks also grew last year. By this the numbers of insider threats were also more. It was because of ease to use mobile tools for gathering and stealing secret information. According to research they found that there were many intellectual property breaches and personally identifiable information breaches in last year.
6	Malware Threats	Rouge antivirus, Malicious links etc	The research by web senses found that malware was became the heart of the cyber threats. There was increase of malware codes and scripts. Last year half of the malwares, which were connected to the web, downloaded additional executables in first 60 seconds only.

Table 19: Websenses information security breaches report worldwide

5.3 SURVEY BY SYMANTEC CORPORATION, SECURITY THREAT REPORT 2013 [92]

Information security threat report 2013 by Symantec Corporation shows that several organizations have been attacked by several advanced attacks. The research has proved that there are so many security breaches have been taken place in recent days of advanced infrastructure of modern networked society. The results of these security breaches are dangerous and could be very harmful in the future too. It is because that the complexity of everything related to technology has been increased. Symantec Corporation found several security breaches last year. From the research some attacks can be categorized as

1. Web related attacks
2. Social engineering attacks
3. Data breaches attacks
4. Malware attacks for instance phishing and spams
5. Mobile and cloud computing attacks

The security breaches were found in all type of organizations. The following Figure 15 shows different type of organizations with percentage of security breaches last year.

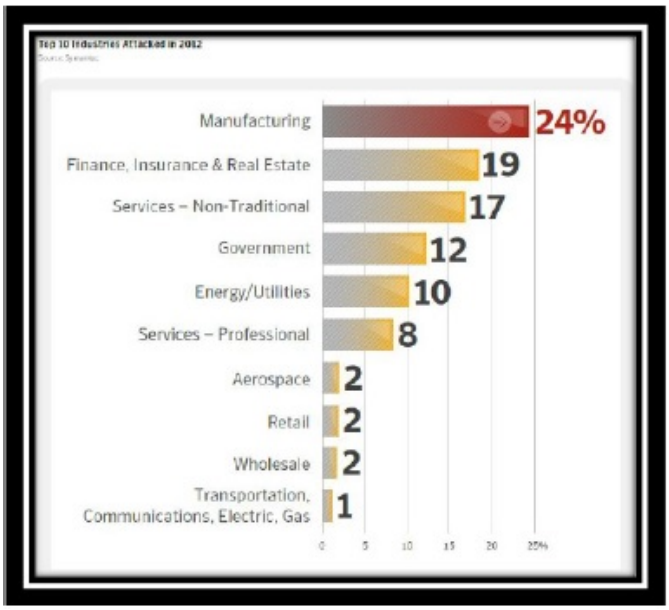

Figure 15: Different types of organizations breached by information security related threats

The Table20 shows some of security breaches examples with its calculation from the survey report.

Table20

Security breaches examples with calculation by Symantec corporation survey 2012 worldwide

SR No.	Security Breach Example	Calculation
1	New vulnerabilities found	5,291 and 415 were mobile vulnerabilities in numbers
2	Average number of identities were breached	604826 in numbers(12 million identities were stolen per month in average)
3	Estimated Global Email Spam in billions	30 billions
4	Estimated Email viruses rate in billions	291 billions
5	Email phishing rate in billions	414 billions
6	Bot zombies in millions	3.4 millions
7	Web attacks per day	247350 millions
8	Mobile malware families increased	58 percent
9	Malicious web domains found in millions	74,000 millions
10	Data breaches found in millions	31 millions
11	Data breaches causes in percentages	Hackers were 40% Accidents were 23% Data Theft/Losses were 23% Insider threats were 8% Unknowns were 6% Frauds were 1%

Table 20: Worldwide information security breaches findings by Symantec corporation in 2012

5.4 SURVEY BY SOPHOS CORPORATION, SECURITY BREACHES THREAT REPORT 2013 [93]

According to Sophos Corporation security breaches threats report 2013, face book and twitter, both were the common websites for exploring security related attacks. Face book was victim of producing new social engineering attacks by 2012. Moreover twitter was victim of delivering direct messages from the compromised accounts. Figure 16 from the survey report shows the

Figure 16: 12 countries which are victim of scams producing

12 top countries which were victim of producing spams worldwide last year with percentage. Another Figure 17 shows the top five safest countries and top five riskiest countries in case of security breaches last year in overall world.

]

Figure 17: Riskiest and safest countries in case of information security breaches in overall world

It has been found during the survey that for example by clicking you tube link of any video, could result in getting infection from the backdoor Trojans. The research shows that the common areas of security breaches in 2012 were cloud computing, mobile computing and use of social networking media. The several examples of security breaches threats are malicious web links, malwares, infected codes, fake antivirus, scams, compromised bank accounts, spams, targeted attacks from Trojan so on.

6 A BALANCED INFORMATION SECURITY MANAGEMENT CONCEPT FOR CKTECK

This chapter covers the concept of balanced information securitymanagement at CKTECK. In this chapter the overall risk management process has been applied on CKTECK's overall risks.The qualatative Risk Management [2] has been followed by the author. The risk management process has been done according to ISO 27001-27005 Risk Management standards. Moreover the author has followed the guidelines by ISACA Risk IT Framework [6] and IT Governance manager's Guide [7]. Furthermore the List of Potential Projects has been listed for the future students as further tasks of the whole case study. This chapter has two sections:

1. Risk Management
2. List Of Potential Projects

6.1 RISK MANAGEMENT

The whole Risk Management process will cover following:

1. Risk Analysis
2. Frequency/Impact Analysis and Risk Map
3. Risk Appetite and Risk Appetite Map
4. Risk Response & Proposed solutions

6.1.1 RISK ANALYSIS

Overall Risk Analysis in BYOD Cloud and Social Media for CKTECK Corporation has already done in Section 4.1.2of Chapter 4. The Risks which will be proceed further in this chapter for Overall Risk Management, are the advanced IT security related risks in BYOD Cloud and Social Media for CKTECK Corporation which have been described in Section 4.1.2.

6.1.2 FREQUENCY/IMPACT ANALYSIS FOR ADVANCE RISKS AND DEFINING RISK MAP

In this section, it has been estimated that how frequent a nature of a particular risk? Moreover, what will be the related consequence of that risk. Advanced IT security related risks have

been taken from Section 4.1.2. The frequency and impact of each risk has been determined in the terms of High/Critical, Medium/Moderate and Low/Insignificant. Red color is used for High/Critical category of risks, Green color is used for Medium/Moderate category of risks and Yellow color is used for low/ insignificant category of risks. The information related to the frequency and impact analysis of each risk can be found in Table 21, Table 22, Table 23, Table 24,Table 25 and Table 26

Following Figure 18 is about the Risk Map of overall risks. It has been made from the results of Frequency/Impact Analysis. In this map this overall risks has been shown according to Risk Categorization.

RISK PROFILE FOR CKTECK RISKS RELATED TO CLOUD , BYOD, SOCIAL MEDIA.

HIGH	C3	C1 B9 B12 B15 SN2 SN17	C8 C25 B2 B14 B27 SN6	C2	SN9	SN13
MEDIUM		B25	C11 B3 SN11 SN12 SN15	SN14 C28 SN1 SN10	C7 C17 B17 B22 SN5 SN8	C21 C5 C23 C29 B23 B4 B5 B7 SN3 SN16
LOW	C6	B19		C4 C19 C22 B13 B21 C26 C32 C34 SN7	C12 C24 SN4 C20 C15 B8 C30 B18 B25	C9 C10 B20 C13 B11 C14 C33 C16 C18 C27 C31 B6 B10 B16 B24 B26
LIKELIHOOD/ CONSEQUENCE	LOW			MEDIUM/MODERATE		HIGH/CRITICAL

Figure 18: Risk Map

6.1.3 RISK APPETITE AND RISK APPETITE MAP

Risk Appetite [2] is "*The broad-based amount of risk a company is willing to accepts in pursuit of its mission (or vision). Risk appetite is the amount of risk an entity is prepared to accept when trying to achieve its objectives*". The Risk Appetite for each risk has been shown in Table 27, Table 28, Table 29, Table 30,Table 31 and 32.

Important factors for Risk Appetite are:

- The enterprise‘s objective capacity to absorb loss
- The culture towards risk taking – cautious or aggressive

Risk Appetite Map has been shown in the Figure 19. Risk Appetite Map has been made from the results of Risk Appetite Process.

<table>
<tr><td>HIGH</td><td>C25
C32</td><td></td><td>B2</td><td></td><td>SN11</td><td>B3
C1
7</td><td>SN9</td><td></td><td>C27
C29
B20</td><td>SN8</td><td>SN6
SN1
5</td><td>B11</td><td>C7
C21</td><td>C8</td></tr>
<tr><td>Medium</td><td rowspan="2">SN17

C3
B21
B27
C6
SN2</td><td rowspan="2">C34
B18

C15
B12
B19
SN10</td><td>B9</td><td></td><td>B20
B22</td><td>C1
6
C2
3
C3
3</td><td>C4
B26
C28</td><td>SN13</td><td>C10
C14
B17</td><td>C2
C5
B7</td><td>SN4</td><td>B16</td><td>C9</td><td>C11
B1</td></tr>
<tr><td>Low</td><td>SN7

B8</td><td>B13</td><td>B26
B30</td><td></td><td>C1
9
B6
B5
B10</td><td>SN16
C13
C1</td><td>B22
B23</td><td>SN3
SN5
B25</td><td>C18

C31
B4
B24
SN1
2</td><td>SN1
C24
SN1
4</td><td>B15</td><td>C12
B14</td></tr>
<tr><td>LIKELIHOOD/
CONSEQUENCE</td><td colspan="2">Low</td><td colspan="9">Medium/Moderate</td><td>High/Critic
al</td></tr>
</table>

Figure 19: Risk Appetite Map for CKTECK’s Overall Risks

6.1.4 RISK RESPONSE & PROPOSED SOLUTIONS

Risk response can be measured with the help of key risk indicators [6]. Key risk indicators are the methods, followed by the Organization as a proposed solution for the upcoming risks. It should be followed to control the frequency and impact of the particular risk. The Risk response be done by following methods, [2], [6].

1. Risk Avoidance
2. Risk Acceptance
3. Risk Sharing / Transfer
4. Risk Reduce/Mitigation

Risk Avoidance:

Risk Avoidance should be proceed when no other risk response is adequate. This is the case when:

- There is no other cost-effective response;
- The risk cannot be shared or transferred;
- The risk is deemed unacceptable by management.

Risk Acceptance:

Risk Acceptance means when no action is required on that risk. The organization is ready to accept the loss related to that particular risk. Acceptance of risk is like when the organization has knowledge that they can accept the loss from its impact.

Risk Sharing/Transfer:

This means reducing the risk by transferring part of it to insurance or outsourcing company. In case of this risk assessment, we have proposed some risks can be shared/transferred. This is because it would be easier and cheaper to share/transfer some of the risk.

Risk Reduction/mitigation:

This means that some action is taken to reduce the risk. Control measures are introduced to minimize the risk of the event happening and if it happens these control measures can reduce the impact to business processes. It can be controlled by proposed solutions.

Figure 20 shows the risks categories from the risk appetite Map 19, which are really unacceptable in CKTECK's Risks Profile. Causes for risks and Key risk indicators for CKTECK have been shown in the Figure 20. The risks has been taken from BYOD, Cloud and Social Media Risks in CKTECK, which are already described in Section 4.1.2 4.1.2 4.1.2. The ideas for finding key risk indicators have been taken from interviews answers in B, C, D, E.

The proposed solutions for some of the CKTECK's risks BYOD, Cloud, Social Media) ,are shown in the Table 33. It shows the particular action which can be taken on that risk and the proposed solution for that risk.

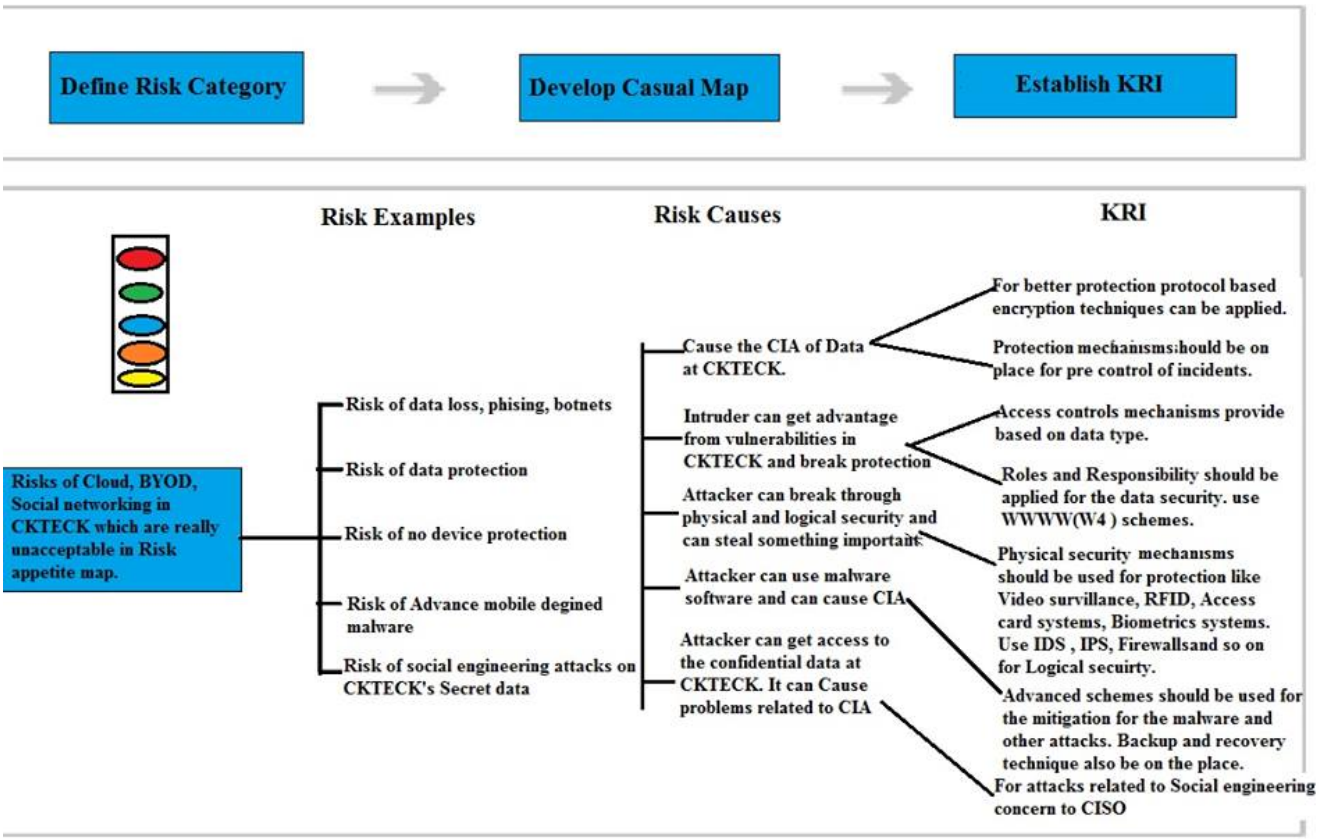

Figure 20: Key Risk Indicators

6.2 LIST OF POTENTIAL PROJECTS

The list of potential projects has been shown below. The students can take these as Challenges and can develop solutions on it. That's how they will be able to learn more about advance IT security Management Concepts.

1. The Overall Risk Management according to ISO 27001-27005 Standards.

   (Hints are: The students can take all risks from CKTECK's (1)BYOD risks 4.1.2,(2) Cloud risks 4.1.2, (3)Social Media risks 4.1.2). Students can choose one or two or all three for gaining better experience with more elaborated risks scenario. For producing overall risk

management plan, the example solutions can be taken from 6.

2. To Define overall plan for the disaster recovery and business continuity for CKTECK's several subsidiaries.

   (Hints are: Students can choose one two subsidiaries of CKTECK and provide solution related to pre, during and post plans in case of natural disasters and other incidents)

3. To write advance information security management policies on Access control policy, Application security policy, Web security policy, Physical security policy, Risk Assessment policy and Audit and Compliance related policy.

   (Hints are: Students can take hint from basic security policy at CKTECK 3.7.2). Students can choose any two and then can try to write advance policies.)

4. To define extended version of CKTECK with more subsidiaries.

   (Hints are: Students can extend CKTECK's subsidiaries with more elaboration. They can take help from 3. Moreover they can find other problems in that areas and propose their solutions too)

5. Survey on Advance Information security breaches on IT security incidents in several organizations and comparison with CKTECK.

   (Hints are: Students can use advance survey reports and can do survey on their basis too. They can make survey questionnaire and can find several outputs of different organizations. Then they can compare it with CKTECK. Students can take help from 5)

6. To plan different access controls on the several stakeholders at CKTECK

   (Hints are: Students can define several access control rights according to the level of any stakeholder at CKTECK. They should consider security of organization in overall manners. For instance students can define which information can be used by which stakeholder and at which level.)

7. To define roles and responsibilities of several stakeholders at CKTECK

(Hints are: Students can define the several roles and responsibilities of different stakeholders at CKTECK, for maintain the information security management. Roles and responsibilities can be defined according to different departments at CKTECK. For instance overall roles of CISO,CEO, CFO and so on)

8. Write several security mechanisms on BYOD security, Social Media Security and Cloud Network Security in CKTECK.

   (Hints are: Students can find several security mechanisms for maintain the BYOD security, Cloud Security and Social Media Security. For example Mobile device management schemes, Security schemes against advance web threats and other related areas)

9. To define Different techniques for educating CKTECK's employees in case of information security management.

   (Hints are: Students can make several rules for the CKTECK employees that what they should do and what they shouldn't do while working. Students can find different ways and techniques of security related education, training and necessary guidance for the employees at CKTECK.)

10. To define Information security economics on the Overall Risk Management

    (Hints are: First students can do risk analysis, countermeasures on any one from (1)BYOD risks 4.1.2,(2) Cloud risks 4.1.2, (3)Social Media risks 4.1.2). After that students can do risk assessment in numbers and monetary terms and can apply any model from *ROSI(Return on security investment) , ROI(Return on investment), NPV(net present value)* financial models. That's how they can motivate the higher authorities at CKTECK for investment on information security mechanisms.

11. Role and importance of Complaince and Audits in CKTECK.

    (Hints are: The students can write about the audits and compliance of CKTECK for advance technologies like BYOD, Cloud or Social Media)

12. Strategy for Incident Management & Response for CKTECK

(Hints are: Students can make plan for several responses plans, investigations for security incidents, forensic analysis, recovery team selection and plans, Management for response and recovery procedures.)

13. An overall Enterprise CKTECK secuirty impact

    (Hints are: Students can write on information security risks of intruders, thefts, fires and floods to software bugs and a variety of IT security issues)

14. To write secure plans on Information Security on joining of new employee at CKTECK

    (Hints are: Students can write on a basic or a multi module planning which will cover all the basic aspects of information security while joining and leaving of any employee)

15. To define secuirty plans for Insider threats at CKTECK

    (Hints are: Students can write on the secuirty aspects on unfaithful employees from CKTECK, from third party, payroll employees at CKTECK, on training employees and so on. Students can write that which important things need to cover from the secuirty point of view.)

16. To define Privacy and Protection at CKTECK

    (Hints are: Students can write guidelines and rules for protecting personal information and respecting the rights of individuals to privacy)

7 DISCUSSIONS, THE FUTURE WORK, CONLUSIONS & FINDINGS

7.1 INTERVIEWS DISCUSSION

7.1.1 *INTERVIEW OF CSO AT VERIZON COMMUNICATIONS, INDIA*

This interview was an Email interview the answers were given by CSO at Verizon communications India. In the Organization they are using their personal cloud network for access the data. After the employees are hired, they provide access to the cloud network according to the roles and responsibilities. They also allowed BYOD, but they have restrictions on it and therefore they haven't faced any financial or reputation loss.

Social media is allowed at the organization but not in working hours. Social media sites are blocked at firewall level. To some extent the users are allowed to use social networking sites on their personal device only.

For the maintenance of security related to BYOD , Cloud and social media they are using some mechanisms:

1. They have completely dedicated cloud network for our org which is not shared with any other org.
2. They have firewall and DMZ created to safeguard our network over internet.
3. BYOD devices on which they allow corporate communication, are secured with "good" software which segregated personal and official data completely and safeguards official data against any kind of attack and coping.
4. Social media sites are blocked at firewall level. All firewall logs are monitored to view exceptions.

In case of incident reporting they have internal incident reporting systems and reaction sites additionally. They are reporting incidents via using networking tools.

In case of security policies they are giving mandatory courses for covering all aspects of policies. There are multiple groups at different operational and governance level who are engaged to

educate users.

7.1.2 INTERVIEW OF *SENIOR SYSTEM ANALYST AT ACCENTURE, OSLO, NORWAY*

The type of interview was an email interview. Questionnaire was sent to a senior system analyst at Accenture Corporation, and the answers were found by an email. From the answers of questions, it has been found that there is no use of personal cloud in the Organization. For the maintenance of information security no one is allowed to use BYOD. The employees are using company's devices only. Moreover they have restriction in the organization of using social media. The organization has its own security policies which are implemented for maintain the information security inside it. The policies examples have been listed above:

- (Data Management) sets out the requirements for the protection of specific Information Assets owned by the Company and those entrusted to it by clients and other third parties.
- (System Security) is a technical Policy that sets out requirements for systems that store and process data, and networks that provide access to data.
- (Acceptable Use of Information, Devices, and Technology) sets out requirements for the way individuals interact with systems and data.
- (External Personnel Access to Company Systems) defines the circumstances under which external personnel can be granted access to Company systems and services.

Furthermore the security awareness training is also given to the employees of the organization. The security trainings which are given to the employees, has been listed above:

1. Security Awareness and protection
2. Ethics and compliance Training

7.1.3 INTERVIEW OF *IT ADMINISTRATOR AT VELOSI, OSLO, NORWAY*

This interview was also an email interview. The answers were given by IT Administrator of Organization Velosi, Oslo, Norway. In the Organization, they have a personal cloud network. They are using cloud network and for the security of cloud network they are using authorization, role based access control and authentication processes. Each employee have their own username and password for the access of cloud network. Moreover all employees have granted different permissions according to their designations. In case of BYOD, they are not allowed to use personal devices at job place but they are using smart devices given by the organization. They are not

using social media within the organization.

When any new employee joins the organization, he or she needs to pass E Learning Exams which are related to information security policy for the organization. That's how they are giving knowledge of security policies to the new employees.

7.1.4 INTERVIEW OF *SYSTEM ANALYST AT TCS, CHICAGO, USA*

In case of Cloud network, they are not using this recent technology of IT. Moreover they have not allowed bringing their own devices at job place. They are using only company enabled devices. They are using just a proxy enabled network in the company. They are not allowed of use of any kind of social networking site inside the organization.

For maintaining BYOD security, there is a guard who manual checks for laptops, USBs , Other portable devices etc. in the carry bags.

For maintaining the security of not using any social media in the company, they are using proxy enabled internet.

If they found any faulty insider person within the organization, they have very strict rules for that. It depends on the severity of the action done by any malicious insider. The punishment could be like a warning, suspension from job at hand, and letter from HR in personal file of malicious insider which can put bad effect and the malicious insider can face difficulties in finding another job.

In case of information security policies, the employees are aware and the organization is giving annually security awareness trainings to the employees which is mandatory for each employee.

7.2 THE FUTURE WORK

This document is an open case study framework for the students. In this the, CKTECK an advanced organization has described and then some of the preliminary tasks are described for the students in 3.8. Later on , some of the solutions examples 4 for that tasks has been given and the overall balanced information security management concept 6 has been shown by the author. Future students can take the tasks descriptions as challenges for them, they can find solutions. That's how the students will be able to learn about actual organizations related situations and they can learn how to handle it. Moreover the students can learn by doing. Learning by doing is very good idea of learning something.

This educational case study describes an organization named CKTECK, its history, its services and products, its customers, its products and areas, its departments, its subsidiaries, several stakeholders, basic information security policy, tasks for the future students, some solution examples. There are some further tasks which have described in Section 6.2 as a List of potential projects, on which the students can work together in the classroom or as an individual project work related task. Students can take that as a real challenge like in the organizations. Afterwards they can try to find several solutions from different ideas. They can add their creativity and knowledge too.

The students can take CKTECK, as a platform to apply other information security related mechanisms in it. In this case study the basic and preliminary Organizations have been described. Students can show overall problems in several areas and departments of CKTCEK. Students can find several loop holes and then they can apply several security mechanisms on several areas. That's how they will become able to know about information security related advanced problems and solutions. The several areas according to ISO 27001 has been already described in Section 4.1.1.

Furthermore, according to the changes in time the new technologies are coming the new case study can be developed. The new and better case study can be developed according to new IT trends, new demands by modern society, new information security related problems, new challenges in the field of information security, new market demands by customers. Then the solutions can be developed according to changed time. It is because that everything is changing very fast. The new developments and changes are taking places very fast in the new modern world. As the things are new, the problems and facts will be also new. Hence this case study will work as an educational tool for the upcoming students in today's time. Because in this case study, the information security problems, challenges, advanced aspects and hot issues, have been shown according to the current time period. In the future everything will be new. Hence, the better new and advanced case study can be developed.

Moreover while developing this kind of document the author have gained a lot of knowledge in the field of information security and related areas in the organization. The author was not aware of environment in the organizations. Hence the author learned a lot from this research for instance, about several stakeholders, the services, the several departments, different roles of stakeholders and so on. This case study is itself worked as an educational tool for the author. The author have learned about several roles of CISO, information security policy, Advanced and hot issues of information security incidents in organization in these days, recent IT trends, current demands in the field of information security, risk management on IT related risks according to ISO 27001 and balanced information security management concept etc. and many more.

7.3 CONCLUSIONS & FINDINGS

From all above it is to be concluded that information security has been become an advanced era of the modern society. There are several security related challenges facing by the advanced organizations in these days. As the problems are new, it is very important to know these problems in advance as risks and should have a solid overall Risk Management Plan to reduce the bad impact of these advanced and new problems. This case study will help the students to learn about latest and advanced problems in the organizations related to information security. Students can learn about advanced risks, threats, vulnerabilities in information security and can learn how to mitigate these. Students can work individually or in groups too on the tasks which have been described in the case study. This educational tool will work as an open study platform for the future students. The case study is related to problems, challenges and solutions according to the current time. In the future new and better case study can be developed according to the new challenges, problems and new technologies. Learning by doing is the best method to teach the students as the author too have worked on several case studies during the study period in several subjects of Msc. in Information Security at HIG. Therefore these case studies are the best method in teaching the students. At last, from this kind of master research, the author too have learned alot on IT secuirty management according to ISO 27001 and advance aspects of information security in the organizations and organization like situations.

Bibliography

[1] Departments and roles, January 13, 2004, Karen Myers , All Rights Reserved, www.KarenLMyers.com http://www.karenlmyers.com/media/attachments/DepartmentsVsRoles.pdf

[2] Lecture Notes of Risk Management 1 course at HIG in IMT. Author: Tone Hoddø Bakås, HIG

[3] AN OVERVIEW OF INFORMATION SECURITY STANDARDS , February 2008 ,© The Government of the Hong Kong Special Administrative Region , http://www.infosec.gov.hk/english/technical/files/overview.pdf

[4] INFORMATION SECURITY, http://en.wikipedia.org/wiki/Information_security

[5] ISO/IEC 27001, Information Security Management System Presented by Daminda Perera 26/07/2008 ,ISO/IEC 27001:27005 Requirements, http://www.daminda.com/downloads/ISO27001.pdf

[6] RISK IT PRACTITIONARY GUIDE BY ISACA, Based on COBIT,ISBN 978-1-60420-116-1,The Risk IT Practitioner Guide, Printed in the United States of America http://raptor1.bizlab.mtsu.edu/s-drive/CAPIGIAN/INFS6300/RiskIT_PG_30June2010_Research.pdf

[7] ITGOVERNANCE, A Manager's Guide to Data Security and ISO27001/ISO 27002 4th edition By Alan Calder & Steve Watkins, ISBN 978 0 7494 5271 1

[8] Addressing cloud computing security issues, Dimitrios Zissis, Dimitrios Lekkas, Future Generation Computer Systems, Volume 28, Issue 3, March 2012, Pages 583-592, ISSN 0167-739X, http://dx.doi.org/10.1016/j.future.2010.12.006, http://www.sciencedirect.com/science/article/pii/S0167739X10002554

[9] Interview:BYOD and the enterprise network, Steve Mansfield-Devine, Computer Fraud & Security, Volume 2012, Issue 4, April 2012, Pages 14-17, ISSN 1361-3723, http://dx.doi.org/10.1016/S1361-3723(12)70031-3, http://www.sciencedirect.com/science/article/pii/S1361372312700313

[10] Social media: opportunity or risk?, Catherine Everett, Computer Fraud & Security, Volume 2010, Issue 6, June 2010, Pages 8-10, ISSN 1361-3723, http://dx.doi.org/10.1016/S1361-3723(10)70066-X http://www.sciencedirect.com/science/article/pii/S136137231070066X

[11] Diez O Silva, "Govcloud: Using Cloud Computing in Public Organizations," Technology and Society Magazine, IEEE , vol.32, no.1, pp.66,72, Spring 2013, doi: 10.1109/MTS.2013.2241473 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6479446&isnumber=6479423

[12] Kandukuri, B.R.; Paturi, V.R.; Rakshit, A., "Cloud Security Issues," Services Computing, 2009. SCC '09. IEEE International Conference on , vol., no., pp.517,520, 21-25 Sept. 2009, doi: 10.1109/SCC.2009.84 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5283911&isnumber=5283890

[13] Kulkarni, G.; Gambhir, J.; Patil, T.; Dongare, A., "A security aspects in cloud computing," Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on , vol., no., pp.547,550, 22-24 June 2012 doi: 10.1109/ICSESS.2012.6269525, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6269525&isnumber=6269390

[14] Sabahi, F., "Cloud computing security threats and responses," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.245,249, 27-29 May 2011 doi: 10.1109/ICCSN.2011.6014715, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6014715&isnumber=6013532

[15] Behl, A., "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," Information and Communication Technologies (WICT), 2011 World Congress on , vol., no., pp.217,222, 11-14 Dec. 2011 doi: 10.1109/WICT.2011.6141247, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6141247&isnumber=6141189

[16] Behl, A.; Behl, K., "An analysis of cloud computing security issues," Information and Communication Technologies (WICT), 2012 World Congress on , vol., no., pp.109,114, Oct. 30 2012-Nov. 2 2012 doi: 10.1109/WICT.2012.6409059, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6409059&isnumber=6409038

[17] Rawai, N.M.; Fathi, M.S.; Abedi, M.; Rambat, S., "Cloud Computing for Green Construction Management," Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on , vol., no., pp.432,435, 16-18 Jan. 2013 doi: 10.1109/ISDEA.2012.107, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6456660&isnumber=6454257

[18] Bouayad, A.; Blilat, A.; El Houda Mejhed, N.; El Ghazi, M., "Cloud computing: Security challenges," Information Science and Technology (CIST), 2012 Colloquium in , vol., no., pp.26,31, 22-24 Oct. 2012 doi: 10.1109/CIST.2012.6388058,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6388058&isnumber=6388042

[19] Gibson, J.; Rondeau, R.; Eveleigh, D.; Qing Tan, "Benefits and challenges of three cloud computing service models," Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on , vol., no., pp.198,205, 21-23 Nov. 2012

doi: 10.1109/CASoN.2012.6412402, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6412402&isnumber=6412367

[20] Abuhussein, A.; Bedi, H.; Shiva, S., "Evaluating security and privacy in cloud computing services: A Stakeholder's perspective," Internet Technology And Secured Transactions, 2012 International Conferece For , vol., no., pp.388,395, 10-12 Dec. 2012 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6470836&isnumber=6470811

[21] Behl, A.; Behl, K., "Security Paradigms for Cloud Computing," Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on , vol., no., pp.200,205, 24-26 July 2012 doi: 10.1109/CICSyN.2012.45, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6274341&isnumber=6274306

[22] Bamiah, M.; Brohi, S.; Chuprat, S.; Brohi, M.N., "Cloud implementation security challenges," Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on , vol., no., pp.174,178, 8-10 Dec. 2012 doi: 10.1109/ICCCTAM.2012.6488093, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6488093&isnumber=6488050

[23] Clour Requirements for a better service, Authors:Eileen Marie Hanna, Nader Mohamed, Jameela Al-Jaroodi ,Published in:Proceeding CCGRID '12 Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012) Pages 787-792 , IEEE Computer Society Washington, DC, USA ©2012 , ISBN: 978-0-7695-4691-9 doi>http://dx.doi.org/10.1109/CCGrid.2012.93, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6217512

[24] AAA, AUTHENTIATION, AUTHORIZATION, ACCOUNTING http://en.wikipedia.org/wiki/AAA_protocol

[25] Knowledge management in the age of cloud computing and Web 2.0: Experiencing the power of disruptive innovations Original Research Article, International Journal of Information Management, Volume 33, Issue 1, February 2013, Pages 160-165, Nabil Sultan,http://dx.doi.org/10.1016/j.ijinfomgt.2012.08.006

[26] Data protection in cloud computing – The Swedish perspective Original Research Article, Computer Law & Security Review, Volume 28, Issue 4, August 2012, Pages 476-480 Dan Jerker B. Svantesson, http://dx.doi.org/10.1016/j.clsr.2012.05.005

[27] The development that leads to the Cloud Computing Business Framework Original Research Article International Journal of Information Management, Volume 33, Issue 3, June 2013, Pages 524-538, Victor Chang, Robert John Walters, Gary Wills, http://dx.doi.org/10.1016/j.ijinfomgt.2013.01.005

[28] Towards secure mobile cloud computing: A survey Original Research Article,Future Generation Computer Systems, Volume 29, Issue 5, July 2013, Pages 1278-1299 Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, http://dx.doi.org/10.1016/j.future.2012.08.003

[29] The Roles of Security and Trust: Comparing Cloud Computing and Banking Original Research Article Procedia - Social and Behavioral Sciences, Volume 73, 27 February 2013, Pages 30-34, Ranjit Bose, Xin (Robert) Luo, Yuan Liu, http://dx.doi.org/10.1016/j.sbspro.2013.02.015

[30] Study on the Security Models and Strategies of Cloud Computing,Original Research Article,Procedia Engineering, Volume 23, 2011, Pages 586-593, Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan,http://dx.doi.org/10.1016/j.proeng.2011.11.2551

[31] Cloud computing as an innovation: Percepetion, attitude, and adoption Original Research Article International Journal of Information Management, Volume 32, Issue 6, December 2012, Pages 533-540 Angela Lin, Nan-Chou Chen, http://dx.doi.org/10.1016/j.ijinfomgt.2012.04.001

[32] Cloud computing and its implications for cybercrime investigations in Australia Original Research Article Computer Law & Security Review, Volume 29, Issue 2, April 2013, Pages 152-163 Christopher Hooper, Ben Martini, Kim-Kwang Raymond Choo, http://dx.doi.org/10.1016/j.clsr.2013.01.006

[33] Privacy and security issues in cloud computing: The role of institutions and institutional evolution Original Research Article Telecommunications Policy, Volume 37, Issues 4–5, May–June 2013, Pages 372-386 Nir Kshetri, http://dx.doi.org/10.1016/j.telpol.2012.04.011

[34] Mobile cloud computing: A survey Original Research Article Future Generation Computer Systems, Volume 29, Issue 1, January 2013, Pages 84-106 Niroshinie Fernando, Seng W. Loke, Wenny Rahayu http://dx.doi.org/10.1016/j.future.2012.05.023

[35] Risk perception and risk management in cloud computing: Results from a case study of Swiss companies Original Research Article International Journal of Information Management, Volume 33, Issue 5, October 2013, Pages 726-733 Nathalie Brender, Iliya Markov, http://dx.doi.org/10.1016/j.ijinfomgt.2013.05.004

[36] Cloud computing security: The scientific challenge, and a survey of solutions Original Research Article Journal of Systems and Software, In Press, Corrected Proof, Available online 18 February 2013 Mark D. Ryan, http://dx.doi.org/10.1016/j.jss.2012.12.025

[37] ISACA , TOP SECUIRTY THREATS TO BANKS IN 2013 https://www.isaca.org/Education/Conferences/Documents/NAISRM-ITGRC-Presentations/221.pdf

[38] NIST(NATIONAL INSTITUTES OF STANDARDS AND TECHNOLOGY, U.S Department Of Commerce) Special Publication 800-37, Revision 1 http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[39] PWC INFORMATION SECURITY BREACHES SURVEY EUROPE 2013 TECHNICAL REPORT, https://www.gov.uk/

government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf

[40] RP Mcafee Threat Prediction 2013 by Mcafee Labs, http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf

[41] Ching-Yung Lin; Wu, L.; Zhen Wen; Hanghang Tong; Griffiths-Fisher, V.; Shi, L.; Lubensky, D., "Social Network Analysis in Enterprise," Proceedings of the IEEE , vol.100, no.9, pp.2759,2776, Sept. 2012, doi: 10.1109/JPROC.2012.2203090 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6249715&isnumber=6269941

[42] Jaakkola, H.; Linna, P.; Henno, J.; Makela, J., "(Social) networking is coming — Are we ready?," MIPRO, 2011 Proceedings of the 34th International Convention , vol., no., pp.1133,1139, 23-27 May 2011, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5967226&isnumber=5967009

[43] Potdar, B.; Nandavadekar, V., "A study of Security Issues Faced and Security Measures Practiced by Citizens of Pune City while working on Social Networking Websites," ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on , vol., no., pp.146,150, 21-23 Nov. 2012 doi: http://dx.doi.org/10.1109/ICTKE.2012.6408545

[44] Mousavi, S.; Demirkan, H., "The Key to Social Media Implementation: Bridging Customer Relationship Management to Social Media," System Sciences (HICSS), 2013 46th Hawaii International Conference on , vol., no., pp.718,727, 7-10 Jan. 2013 doi: 10.1109/HICSS.2013.531 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6479920&isnumber=6479821

[45] Chandramouli, R., "Emerging social media threats: Technology and policy perspectives," Cybersecurity Summit (WCS), 2011 Second Worldwide , vol., no., pp.1,4, 1-2 June 2011 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978791&isnumber=5978775

[46] The impact of polices on government social media usage: Issues, challenges, and recommendations Original Research Article Government Information Quarterly, Volume 29, Issue 1, January 2012, Pages 30-40 John Carlo Bertot, Paul T. Jaeger, Derek Hansen, http://dx.doi.org/10.1016/j.giq.2011.04.004

[47] Author:Pradeep K. Atrey, The University of Winnipeg, Winnipeg, MAN, Canada, Proceeding MiFor '11 Proceedings of the 3rd international ACM workshop on Multimedia in forensics and intelligence Pages 13-18 ACM New York, NY, USA ©2011, table of contents ISBN: 978-1-4503-0987-5 doi>http://dx.doi.org/10.1145/2072521.2072525

[48] Social networking searching and privacy issues Original Research Article Information Security Technical Report, Volume 16, Issue 2, May 2011, Pages 74-78 Man Qi, Denis Edgar-Nevill http://dx.doi.org/10.1016/j.istr.2011.09.005

[49] The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption Original Research Article Interacting with Computers, Volume 22, Issue 5, September 2010, Pages 428-438 Dong-Hee Shin http://dx.doi.org/10.1016/j.intcom.2010.05.001

[50] Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia Original Research Article Computers in Human Behavior, Volume 28, Issue 6, November 2012, Pages 2366-2375, Norshidah Mohamed, Ili Hawa Ahmad http://dx.doi.org/10.1016/j.chb.2012.07.008

[51] Mobile social networking middleware: A survey Review Article Pervasive and Mobile Computing, Volume 9, Issue 4, August 2013, Pages 437-453 Paolo Bellavista, Rebecca Montanari, Sajal K. Das http://dx.doi.org/10.1016/j.pmcj.2013.03.001

[52] Privacy Issues in Mobile Social Networks Original Research Article Procedia Computer Science, Volume 10, 2012, Pages 672-679 Racha Ajami, Nabeel Al Qirim, Noha Ramadan http://dx.doi.org/10.1016/j.procs.2012.06.086

[53] Anti-social networking: exploiting the trusting environment of Web 2.0 Original Research Article Network Security, Volume 2008, Issue 11, November 2008, Pages 4-7 Steve Mansfield-Devine, http://dx.doi.org/10.1016/S1353-4858(08)70127-2

[54] Forensic analysis of social networking applications on mobile devices Original Research Article Digital Investigation, Volume 9, Supplement, August 2012, Pages S24-S33 Noora Al Mutawa, Ibrahim Baggili, Andrew Marrington, http://dx.doi.org/10.1016/j.diin.2012.05.007

[55] Online Social Networking for Quality of Life Original Research Article Procedia - Social and Behavioral Sciences, Volume 35, 2012, Pages 713-718 Noorriati Din, Saadiah Yahya, Raja Suzan, Raja Kassim http://dx.doi.org/10.1016/j.sbspro.2012.02.141

[56] All about me: Disclosure in online social networking profiles: The case of FACEBOOK Original Research Article Computers in Human Behavior, Volume 26, Issue 3, May 2010, Pages 406-418 Amanda Nosko, Eileen Wood, Seija Molema, http://dx.doi.org/10.1016/j.chb.2009.11.012

[57] Key quality factors affecting users' perception of social networking websites Original Research Article Journal of Retailing and Consumer Services, Volume 20, Issue 1, January 2013, Pages 120-129 Abida Ellahi, Rahat H. Bokhari, http://dx.doi.org/10.1016/j.jretconser.2012.10.013

[58] Special section on Security and Social Networking Computer Communications, Volume 35, Issue 1, 1 January 2012, Page 47 Melek Önen, Thorsten Strufe http://dx.doi.org/10.1016/j.comcom.2011.10.009

[59] The impact of Arab cultural values on online social networking: The case of Facebook Original Research Article Computers in Human Behavior, Volume 28, Issue 6, November

2012, Pages 2387-2399 Khaled Saleh Al Omoush, Saad Ghaleb Yaseen, Mohammad Atwah Alma'aitah http://dx.doi.org/10.1016/j.chb.2012.07.010

[60] The threats of social networking: Old wine in new bottles? Original Research Article Information Security Technical Report, Volume 16, Issue 2, May 2011, Pages 38-43 George R.S. Weir, Fergus Toolan, Duncan Smeed, http://dx.doi.org/10.1016/j.istr.2011.09.008

[61] Living a private life in public social networks: An exploration of member self-disclosure Original Research Article Decision Support Systems, Volume 55, Issue 3, June 2013, Pages 661-668 Rui Chen, http://dx.doi.org/10.1016/j.dss.2012.12.003

[62] Social networking in the workplace Network Security, Volume 2011, Issue 10, October 2011, Page 20 http://dx.doi.org/10.1016/S1353-4858(11)70109-X

[63] INFORMATION SECURITY THREAT REPORT BY WEBSENSES, http://www.websense.com/assets/reports/websense-2013-threat-report.pdf

[64] Security review: the past year Original Research Article Computer Fraud & Security, Volume 2013, Issue 1, January 2013, Pages 5-11 Steve Mansfield-Devine http://dx.doi.org/10.1016/S1361-3723(13)70006-X

[65] Dhami, A.; Agarwal, N.; Chakraborty, T.K.; Singh, B.P.; Minj, J., "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook," Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.465,469, 22-23 Feb. 2013 doi: 10.1109/IAdCC.2013.6514270 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6514270&isnumber=6506800

[66] Chapter Ist of book managing the human factor in information security, by David Lacy. Copyright @ 2009, John Wiley & Sons Ltd, The Atrium, Southern Gate , Chichester,West Sussex PO19 8SQ, England

[67] IT Enabled Services 2013, pp 217-227 Real Name Social Networking Services and Risks of Digital Identity Yohko Orito, http://download.springer.com/static/pdf/943/chp%253A10.1007%252F978-3-7091-1425-4_13.pdf?auth66=1385695303_9e8b975fe556ed1d3c71fd901974778d&ext=.pdf

[68] Perceived risks and risk management of social media in an organizational context Juha Munnukka, Pentti Järvi, Electronic Markets The International Journal on Networked Business © Institute of Information Management, University of St. Gallen 2013 http://dx.doi.org/10.1007/s12525-013-0138-2, http://download.springer.com/static/pdf/369/art%253A10.1007%252Fs12525-013-0138-2.pdf?auth66=1385695390_0d0a477479479d848248170c9eed50da&ext=.pdf

[69] SANS INSTITUTE WHITEPAPER, http://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749

[70] A SECURITY REPORT ON INFORMATION SECURITY SHAKE UP, SBIC special Report RSA, The Security Division of EMC http://www.google.no/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=6&ved=0CEUQFjAF&url=http%3A%2F%2Fwww.emc.com%2Fcollateral%2Findustry-overview%2Fh11391-rpt-information-security-shake-up.pdf&ei=0nANUu3gL4OU4ATHgoD4DA&usg=AFQjCNGn2HXL741gw0itIx7HyInGd7u2Pg&sig2=zrB6eoqxU9m6ohycUv-QSg

[71] Scarfo, A., "New Security Perspectives around BYOD," Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on , vol., no., pp.446,451, 12-14 Nov. 2012 doi: 10.1109/BWCCA.2012.79 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6363095&isnumber=6363025

[72] 2013 Trends and Strategies Costello, Tom ; Prohaska, Beverly IT Professional ,Volume:15, Issue: 1 http://dx.doi.org/10.1109/MITP.2013.5 Publication Year: 2013 , Page(s): 64

[73] Sangani, K., "BYOD to the classroom," Engineering & Technology , vol.8, no.3, pp.42,45, April 2013 doi: 10.1049/et.2013.0304 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6495438&isnumber=6495435

[74] Hayes, J., "The device divide," Engineering & Technology , vol.7, no.9, pp.76,78, October 2012 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6411645&isnumber=6330927

[75] Miller, K.W.; Voas, J.; Hurlburt, G.F., "BYOD: Security and Privacy Considerations," IT Professional , vol.14, no.5, pp.53,55, Sept.-Oct. 2012 doi: 10.1109/MITP.2012.93 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6320585&isnumber=6320581

[76] WHY THE BYOD BOOM IS CHANGING HOW WE THINK ABOUT BUSINESS IT, By:Oliver Richard, Engineering & Technology ,Volume:7 , Issue: 10, Publication Year: 2012 , Page(s): 28

[77] Bring your own device (BYOD) with Cloud 4 education Author: Ruth G. Lennon Letterkenny Institute of Technology, Letterkenny, Co. Donegal, Ireland Proceeding SPLASH '12 Proceedings of the 3rd annual conference on Systems, programming, and applications: software for humanity Pages 171-180 , ACM New York, NY, USA ©2012 , ISBN: 978-1-4503-1563-0 doi>http://dx.doi.org/10.1145/2384716.2384771

[78] Bring your own device, securely Authors: Alessandro Armando, Fondazione Bruno Kessler, Trento, Italy Gabriele Costa, Luca Verderame Università degli Studi di, Genova, Genova, Italy Alessio Merlo Università E-Campus, Novedrate, Italy, Proceeding SAC '13 Proceedings of the 28th Annual ACM Symposium on Applied Computing Pages 1852-1858 ACM New York, NY, USA ©2013 ISBN: 978-1-4503-1656-9 doi>http://dx.doi.org/10.1145/2480362.2480707

[79] Gordon Thomson, BYOD: enabling the chaos, Network Security, Volume 2012, Issue 2, February 2012, Pages 5-8, ISSN 1353-4858, http://dx.doi.org/10.1016/

S1353-4858(12)70013-2 http://www.sciencedirect.com/science/article/pii/S1353485812700132

[80] The security implications of BYOD Original Research Article Network Security, Volume 2013, Issue 4, April 2013, Pages 12-13 Brian Tokuyoshi, http://dx.doi.org/10.1016/S1353-4858(13)70050-3

[81] BYOD security challenges: control and protect your most sensitive data Original Research Article Network Security, Volume 2012, Issue 12, December 2012, Pages 5-8 Bill Morrow, http://dx.doi.org/10.1016/S1353-4858(12)70111-3

[82] Author: Siv Hilde Houmb, Lecture Notes of Information Security Economics, HIG subject for IMT at GUC

[83] Information security policy in small education organization,2009 Article Authors: Wasim A. Al-Hamdani Kentucky State University, Frankfort, KY, Wendy D. Dixie Kentucky State University, Frankfort, KY Proceeding InfoSecCD '09 2009 Information Security Curriculum Development Conference, Pages 72-78 ACM New York, NY, USA ©2009 , table of contents ISBN: 978-1-60558-661-8 doi http://dx.doi.org/10.1145/1940976.1940991

[84] Sample Information Secuirty Policy by Credit Suisse Group, Version 2.0

[85] Bringing IT out of the shadows Original Research Article Network Security, Volume 2013, Issue 4, April 2013, Pages 5-11 Richard Walters http://dx.doi.org/10.1016/S1353-4858(13)70049-7

[86] The state of information security Original Research Article Network Security, Volume 2012, Issue 7, July 2012, Pages 9-11 Mike Potts, http://dx.doi.org/10.1016/S1353-4858(12)70064-8

[87] About BYOD, By IBM Corporation http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html

[88] BYOD benifits http://www.mcpc.com/benefits-of-BYOD

[89] Sample Information Security Policy by DTI, Published by the Department of Trade and Industry, © Crown Copyright. URN 06/1647

[90] Roles And Responsibilities of CISO, California Office of Information Security and Privacy Protection, Guide for the Roles and Responsibilities of an Information Security Officer Within State Government April 2008, http://www.cio.ca.gov/OIS/Government/documents/pdf/ISO_Roles_Respon_Guide.pdf

[91] ISACA & TCS, BYOD Security and security breaches in BYOD, Published on 2/23/2013. http://www.theiiat.or.th/media/km/thumbnail/47/130226142847/BYOD%20-%20ISACA%20-%20Final%2020130223%20Vorapoj%20Lookmaipun.pdf

[92] SURVEY BY SYMANTEC CORPORATION, Internet Security Threat Report 2013, Volume 18,2012 Trends, Published April 2013 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[93] SURVEY BY SOPHOS CORPORATION

http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

A TABLES OF RISK MANAGEMENT PROCESS

Table21

S.No	Ref	Risk Category	Risk Description	Rating
1	C2	C2: Risk related to big data storage in cloud is itself a risk [11]	Because of less security of personal data over cloud environment will be critical risk for the organisation	High/Critical
2	C5	C5: Risk of Low availability of data [11] [21]	The cloud network in CKTECK can be compromised by the denial of service attacks.	High/Critical
3	C7	C7: Risk of data loss, phishing, botnets [13]	These type of risks always there because of Intruder in the cloud.	High/Critical
4	C9	C9: Risk of data protection [13]	In these days when organisation opting the cloud services for the communication for their own purpose. High level risks always there.	High/Critical
5	C10	C10: Risk of data leakage [13] [14]	Cloud has advantages and disadvantages in organisation data leakage always there.	High/Critical
6	C13	C13: Risk of malicious outside attacks [15]	Risks related to Malicious attacks always active in Cloud that's why its active in nature.	High/Critical
7	C14	C14: Risk regarding loss of control on data location [15]	Due to flexibility of cloud network the control is very difficult and always chance of risk in cloud.	High/Critical
8	C16	C16: Risk of unawareness by cloud providers to hosted services [18]	This is high because the technology readily changing and chance of such risk is always there.	High/Critical
9	C17	C17: Risk of virtual machines and virtualization [18] [22]	Virtualization in cloud is also a risk due to expandability. Because the boundary are not limited always.	High/Critical
10	C18	C18: Risk of data sanitization [20]	It is a serious risk in the CKTECK cloud infrastructure. In simple words can we imagine that what will happen when the cloud service is terminated? Moreover what will happen to the data of the user of CKTECK.	High/Critical
11	C21	C21: Service Hijacking risk [21]	By this, the attackers can gain access to the services of CKTECK. It is because the cloud is not strongly secured	High/Critical
12	C23	C23: Risk of insecure API's in cloud [22]	API's are designed to provide protection against accidental as well as malicious attacks. The main features of API's are encryption and monitoring of the activities. Attackers are also very smart in these days. They can use several methods for ending keys.	High/Critical
13	C27	C27: Risk of Improper Identity management [22]	This is also a high level risk because Identity management is the base of CIA, which is the base of information security. If is not managed properly with granted access then it may harm the CKTECK cloud network.	High/Critical
14	C29	C29: Risk of privileged user access [35]	In cloud the chance of malicious attack for taking the access in authorized manner. It cloud be a bigger risk to the organisation	High/Critical

Table 21: Frequency/Impact Analysis for each risk

Table22

15	C31	C31: Risk of hardware & software failure due to natural disasters [22]	These types of risks are once in a blue moon type but when it comes than it unstoppable. so in such manner this also critical in nature.	High/Critical
16	C33	C33: Risk in recovery from disasters [035]	In case of no prior planning of disaster recovery and backup procedures by CKTECK	High/Critical
17	B1	B1: Risk of device lost or stolen [71]	In BYOD technology the chance of device the very less in nature but if somebody miss such device with sensitive information then it comes as a bigger threat for the CKTECK.	High/Critical
18	B4	B4: Risk of data tampering [71]	If the alteration of data occur in CKTECK BYOD environment than the chance of critical risk will be there.	High/Critical
19	B5	B5: Risk of data unavailability [71]	Unavailability of data is also a big threat to the information security organisation like CKTECK.	High/Critical
20	B6	B6: Risk of unmanaged and untrusted devices on CKTECK network [74]	The mobile devices sometimes not under a full control of the enterprise. If these are untrusted and unmanaged than it comes as a big risk for the CKTECK organization.	High/Critical
21	B7	B7: Risk of Malware Migration [75]	In BYOD, migrating malwares from the devices to the whole network of CKTECK and its machines too. It comes as a high risk for the CKTECK	High/Critical
22	B10	B10: Risk of no-protection of network traffic [80]	If the devices at CKTECK are without protection mechanisms in proper place which can secure network traffic then there is always risk to the corporate information. this can be dangerous for CKTECK.	High/Critical
23	B11	B11: Risk of no device protection [80]	This risk comes into place when the CKTECK's employee as the owner of the device is not using it directly. Hence this is a big risk for CKTECK.	High/Critical
24	B16	B16: Risk of advanced mobile designed malware [81]	When employees at CKTECK install the applications on the personal devices including games, music, media, social networking and so on then there is always a risk of viruses, bots and other mobile designed advanced malwares. This can be big risk for CKTECK.	High/Critical
25	B17	B17: Risk of exploiting vulnerabilities in mobile systems [81]	When the employees of CKTECK have no control in place for the usage of the mobile devices and when the employees are ignoring existing security policies then the vulnerabilities of the devices can be exploited easily by the hackers or false persons. In case of BYOD this will be the critical one.	High/Critical

Table 22: Frequency/Impact Analysis for each risk

Table23

26	B20	B20: Risk of insecure antivirus [81]	Even in today's anti viruses are not fully effective for advanced malwares. For instance man in the browses attack (MitB) sits in web browser between the user and the website. It can alter and change the data. Additionally it is putting web based corporate data on the risk. It is risky for CKTECK too.	High/Critical
27	B22	B:22 Risk of data extraction can be done easily by intruders [81]	Data in the devices is remained in cleared text format which can be extracted easily by the intruders and advanced malwares. Moreover the cut, copy, paste, and deleted data is remained in clear text form. Hence it can be misused by smart hackers. highly risky for CKTECK.	High/Critical
28	B23	B23: Risk of new culture of hacking techniques [86]	It can leads to data breach. CIA of CKTECK can be disturbed with such risks.	High/Critical
29	B24	B24: Risk of industrialized attacks [86]	Industrialized attacks are related to the world of cyber attacks. Recent related example is SpyEye banking malware. such kind of attack can be dangerous for CKTECK as well.	High/Critical
30	B26	B:26 Risk of fully automated attacks [86]	Automated attacks are the attacks which are designed by the hackers for the automatic migration of malwares into the system.	High/Critical
31	SN3	SN3: Risk of unauthorized access to data by hackers [49]	By the use of social networking sites by CKTECK employees, hackers can get chance to easily gain unauthorized attempt and access to the private and confidential data of corporation CKTECK. can cause as critical risk.	High/Critical
32	SN5	SN5: Risk of getting private conversations of the CKTECK [49]	This can be leaked to the malicious insider, which can get username and password. Later he can misuse it. and lead to a bigger risk for CKTECK.	High/Critical
33	SN8	SN8: Risk of online identity theft and identity misuse [50] [56] [59] [60] [64]	Online identity can be comprised with advanced methods.. Therefore results may be highly dangerous for instance money theft from digital accounts, identity misuse in cybercrimes and so on.	High/Critical
34	SN9	SN9: Risk of online scams, viruses, malwares, network intrusions and spywares [50] [53] [64]	Social networking sites are victim of insecure transfers. this leads to a dangerous risk for CKTECK.	High/Critical
35	SN13	SN13: Cybercrime risks and cyber threats [54] [63] [61] [63] [64]	It can be emerge through the cyber threats	High/Critical
36	SN16	SN16: Risk of fake antivirus [64]	Fake antivirus takes file hostage and then encrypts them and requires the employees to wire the money. It may be result in big money loss to the Corporation CKTECK.	High/Critical

Table 23: Frequency/Impact Analysis for each risk

Table24

37	C1	C1: Risk of storing personally identifiable information [11]	Because of information can be assessed and operated by cloud provider CKTECK. Therefore it can be result in misuse of the important and sensitive information of CKTECK in the cloud.	Medium/Moderate
38	C4	C4: Risk of low confidentiality of data [11]	The cloud provider has risk regarding accessing the data because the encryption is not strong enough in the cloud.	Medium/Moderate
39	C8	C8: Risk of data privacy [13]	Data and information of CKTECK are not remains private because it is also even stored outside the country.	Medium/Moderate
40	C11	C11: Risk of insider threats and malicious insiders [15] [22]	Some reasons are lack of transparency, processes to hire new employees, keeping data at different locations, relations to the third parties, casual hackers this leads to the risk.	Medium/Moderate
41	C12	C12: Risk of lost of data through migration of data [15]	Due to multi subsidiary of CKTECK this type of risk always there.	Medium/Moderate
42	C19	C19: Risk of difficult backup procedure [20]	The backup procedure in CKTECK's cloud environment could be difficult because of data storage at unknown locations.	Medium/Moderate
43	C20	C20: Risk of multi tenancy property of cloud [21] [22]	Cloud works on multi tenancy model which means that cloud services are scalable in the shared infrastructure for CKTECK.	Medium/Moderate
44	C22	C22: Risk of repudiation of the information [21]	Sometimes cloud provider can't claim that the information transmitted was correct or not. this leads a risk in some way.	Medium/Moderate
45	C24	C24: Risk of improper key management in backup [22]	Improper key management creates difficulty in maintaining the backup procedures for the CKTECK employees.	Medium/Moderate
46	C25	C25: Risk related to Data Governance and Compliance [22]	Non-compliance with laws, regulations, or policies of the CKTECK	Medium/Moderate
47	C26	C26: Risk in SLA [22]	There is always a risk for CKTECK because of lack of trusts in the clients and loss of data governance.	Medium/Moderate
48	C28	C28: Risk of compliance and data location [35]	Data location is a big issue in the cloud computing related to the privacy regulations in different jurisdictions.	Medium/Moderate
49	C30	C30: Risk in investigation support and forensic investigation [35]	risk for CKTECK employees of difficulty in the forensic investigation too because of data at several unknown locations.	Medium/Moderate
50	C32	C32: Risk in unavailability of cloud network [35]	There could be chances of the risk of unavailability of services. This leads to risk	Medium/Moderate
51	C34	C34: Risk in mitigation of cloud service in case of business continuity [35]	Improper performance checking, improper profitability, improper local storage capacity, irregular backups and data on local services, improper contingency plans	Medium/Moderate

Table 24: Frequency/Impact Analysis for each risk

Table25

52	B2	B2: Risk of attacks from the devices [71]	Nature of the internet is insecure. There is always a risk of device attacks while using internet. Hence, the security of the devices can be compromised because of this. This is risky for the CKTECK.	Medium/Moderate
53	B3	B3: Risk of data Loss [71] [85]	when the unauthorized movement of the data which occurs outside the control environment of the CKTECK network. It may be result in data loss.	Medium/Moderate
54	B8	B8: Risk of no control on data on personal devices [75]	When the CKTECK's information migrates to the personal devices then after that there is no control on that information from the organization side for instance CKTECK's data becomes no longer under control	Medium/Moderate
55	B9	B9: Risk of disclosure of private and personal data due to togetherness of storage of personal and corporation data [75]	When the personal and corporate data of CKTECK's employees is stored on same device then it would be very difficult for CKTECK to maintain security	Medium/Moderate
56	B12	B12: Risk of uncontrolled device and enforcing compliance [80]	By using BYOD at CKTECK, there is always a risk that how to enforcing compliances properly with the guidelines of the corporate when employee is on the move.	Medium/Moderate
57	B13	B13: Risk of Unknown IP address [80]	It is a possibility when The employees in CKTECK don't know that who is using a particular IP address and the identity isn't being used as a element of the policy.	Medium/Moderate
58	B14	B14: Risk of advanced threats [81]	Due to the enhancement of new technologies, the new security related threats have been emerged too for instance key loggers, malwares, cyber attacks, botnets etc.	Medium/Moderate
59	B15	B15: Risk of Insider threats [81]	malicious employee in CKTECK can steal corporation secrets, intellectual property, and sensitive customer's information	Medium/Moderate
60	B18	B:18 Risk of no proper security standards for mobile devices [81]	Security standards like authentication, SSL encryption, IPS, firewalls etc are not always secure against advanced malwares and there the perfectly secure mobile security standards have not been discovered. This leads a high risk to the enterprise CKTECK.	Medium/Moderate
61	B21	B21: Risk of no control on users downloads [81]	When administrator have no control on internet usage of the employee this leads to risk	Medium/Moderate
62	B25	B25: Risk of employee Misuse and abuse [86]	When information is misused by employee by restricting policies	Medium/Moderate
63	B27	B27: Risk of mobile threats [40]	Mobile threats are like mobile worms on victims, malicious mobile applications, mobile mal- wares, Sms spams, smishing and vishing	Medium/Moderate

Table 25: Frequency/Impact Analysis for each risk

Table26

64	SN1	SN1: Risk of disclosure of private information on the sites [48] [60]	When the personal information on social media site miscued by malicious person	Medium/Moderate
65	SN2	SN2: Risk of malicious third party [48]	Malicious third party on social media site can misuse the organisation information	Medium/Moderate
66	SN4	SN4: Risk of gaining access to the secret information of organization CKTECK [49]	When any malicious person wants to breach the security and able to gain access on the confidential information.	Medium/Moderate
67	SN6	SN6: Risk of social phishing [50]	Its a risks from the phishers site. which are also related with social media risks.	Medium/Moderate
68	SN7	SN7: Risk of inability to control the information regarding user posts in Social Networking [50]	When private chat on social media is misused by unauthorized person	Medium/Moderate
69	SN10	SN10: Risk of location tracking from mobile social networking [53]	When the location tracked by malicious person.	Medium/Moderate
70	SN11	SN11: Risk of data manipulation [54] [69]	When attacker can modify the data through malware or any other malicious application	Medium/Moderate
71	SN12	SN12: Data retrieving risk [54]	Data can be retrieved the data by Social network sites	Medium/Moderate
72	SN14	SN14: Risk of data misuse and abuse [54]	In such problem the malicious person can misuse the information from SN website.	Medium/Moderate
73	SN15	SN15: Risk of social engineering attacks on CKTECK's secret data [60] [63]	These types of attacks are common in nature. and leads to reputation loss and all	Medium/Moderate
74	SN17	SN17: Other miscellaneous risks [62]	Risk of violation of confidentiality of CKTECK Bandwidth diminished	Medium/Moderate
75	C3	C3: Risk of auditing and compliance [11] [21]	Non-compliance with laws, Regulations, or policies. Risk from bad auditing.	Low/Insignificant
76	C6	C6: Risk in Secure socket layer [13]	Secure socket layer in the CKTECK's cloud can be vulnerable due to the man in the middle attack.	Low/Insignificant
77	C15	C15: Risk of no standard security specifications and loss of control [18] [21]	There is no standard for cloud security.	Low/Insignificant
78	B19	B19: Risk of no visibility to the end users [81]	No visibility to the BYOD device.	Low/Insignificant

Table 26: Frequency/Impact Analysis for each risk

Table27

S. No	Ref	Risk Category	On Basis of CIA			Rating
			Confidentiality	Integrity	Availability	
1	C2	C2: Risk related to big data storage in cloud is itself a risk [11]	Confidentiality can be harm at higher level	Can make loss of information and attacker can put some falsifying information to mislead the normal organisational process	Highly effed because its difficult to put cryptographic controls than hacker can make data unavailable.	Unacceptable
2	C5	C5: Risk of Low availability of data [11] [21]	No changes	No changes	Effect on Availability	Unacceptable
3	C7	C7: Risk of data loss, phishing, botnets [13]	Effect on confidentiality	With such attacks integrity can also damage	With such advanced risks the availability will also damaged	Really unacceptable
4	C9	C9: Risk of data protection [13]	confidentiality is critical against the malicious software (malware), spy ware, spam and phishing attacks.	Integrity is also critical against the malicious software (malware), spyware, spam and Phishing attacks.	Availability need full protection against malicious software (malware), spyware, spam and phishing attacks.	Really unacceptable
5	C10	C10: Risk of data leakage [13] [14]	Data leakage mainly effect on confidentiality	No changes	Availability effects to some extent	Unacceptable
6	C13	C13: Risk of malicious outside attacks [15]	Try to effect the confidentiality with advanced techniques of hacking	Integrity of data will effect by the outsider.	No effect	Acceptable(with advanced techniques of defence)
7	C14	C14: Risk regarding loss of control on data location [15]	No effect	No effect	Will be much effected	Unacceptable
8	C16	C16: Risk of unawareness by cloud providers to hosted services [18]	No effect	No effect	No effect	Acceptable
9	C17	C17: Risk of virtual machines and virtualization [18] [22]	No effect	Integrity of data will be effected in virtual environment	Availability will not effect with high loss	Acceptable
10	C18	C18: Risk of data sanitization [20]	No effect	No effect	Highly effected in such type of risk condition	Unacceptable
11	C21	C21: Service Hijacking risk [21]	High risks for the confidentiality perspective	Integrity will also effects	Availability will decreases throughout the down time	Really unacceptable

Table 27: Risk Appetite

Table28

12	C23	C23: Risk of insecure API's in cloud [22]	No effects on confidentiality	Integrity also secure in such	Less chance for the unavailability	Acceptable
13	C27	C27: Risk of Improper Identity management [22]	Confidentiality will effect by unauthorized person	Modification chance will be there	No effect	Unacceptable
14	C29	C29: Risk of privileged user access [35]	Confidentiality will effect by gaining privileged access by insider threats	Modification will also be there	No effect	Unacceptable
15	C31	C31: Risk of hardware & software failure due to natural disasters [22]	No effect	No effect	Highly effected	Unacceptable
16	C33	C33: Risk in recovery from disasters [035]	No effect	No effect	No effect	Acceptable
17	B1	B1: Risk of device lost or stolen [71]	With loss the confidentiality will be highly effected	No effect	Highly effected	Really unacceptable
18	B4	B4: Risk of data tampering [71]	Confidentiality breaches	Integrity of data will surely effected	To some extent	Unacceptable
19	B5	B5: Risk of data unavailability [71]	No effect	No effects	Highly effected	Acceptable
20	B6	B6: Risk of unmanaged and untrusted devices on CKTECK network [74]	Breach of confidentiality	No effect	No effect	Acceptable
21	B7	B7: Risk of Malware Migration [75]	Confidentiality effected	Could be there in this case	Unavailability of data can be there	Unacceptable
22	B10	B10: Risk of no-protection of network traffic [80]	It effects on confidentiality	No effect	Will be surpassed	Acceptable
23	B11	B11: Risk of no device protection [80]	Confidentiality will be highly effected	Data without protected mode could be modified	Unavailability of system will be there without protection mechanism	Really unacceptable.
24	B16	B16: Risk of advanced mobile designed malware [81]	Can cause to the confidentiality of the data	With advanced design malware it can effect the integrity with advanced breakage methods	Malware with such BYOD technology can halt the overall system and unavailability of the data will be there.	Really unacceptable
25	B17	B17: Risk of exploiting vulnerabilities in mobile systems [81]	Breach of confidentiality	Integrity can also be effected	Unavailability of services can be there.	Unacceptable

Table 28: Risk Appetite

Table29

26	B20	B20: Risk of insecure antivirus [81]	Effects confidentiality	Effects too some extent	Unavailability can be effected by crash of hardware and software without antivirus.	Unacceptable.
27	B22	B:22 Risk of data extraction can be done easily by intruders [81]	Breach of confidentiality will be there	Effects on integrity of the data	No effects on unavailability	Acceptable
28	B23	B23: Risk of new culture of hacking techniques [86]	Too some extant	To some extent	No effect	Acceptable
29	B24	B24: Risk of industrialized attacks [86]	Breach of confidentiality will be high in nature	Integrity of data will also be highly effected	No effects	Unacceptable
30	B26	B:26 Risk of fully automated attacks [86]	Too some extant	To some extent	No effect	Acceptable
31	SN 3	SN3: Risk of unauthorized access to data by hackers [49]	Breach of confidentiality	By unauthorized access hacker can change or modified the data	Hacker can make the data unavailable	Unacceptable
32	SN 5	SN5: Risk of getting private conversations of the CKTECK [49]	Effect on confidentiality	Effect on integrity of the data	Intruder can make the data unavailable	Unacceptable
33	SN 8	SN8: Risk of online identity theft and identity misuse [50] [56] [59] [60] [64]	Effect on confidentiality	No effect	Make the data unavailable	Unacceptable
34	SN 9	SN9: Risk of online scams, viruses, malwares, network intrusions and spywares [50] [53] [64]	No much effected	To some extent	Effect on unavailability of data	Acceptable
35	SN 13	SN13: Cybercrime risks and cyber threats [54] [63] [61] [63] [64]	Breach of confidentiality	To some extent	Make data unavailable to some extent	Acceptable
36	SN 16	SN16: Risk of fake antivirus [64]	Breach to some extent	Breach to some extent	Breach to some extent	Acceptable
37	C1	C1: Risk of storing personally identifiable information [11]	Risks of confidentiality to some extent	No issues with integrity	Sometimes data can be unavailable	Acceptable
38	C4	C4: Risk of low confidentiality of data [11]	Due to lack in cryptographic technique breach of confidentiality will be there	Modification of data can be possible	No effect	Acceptable
39	C8	C8: Risk of data privacy [13]	Confidentiality loss	Modification can be possible	Unavailability of data can be possible because long distance sharing	Really unacceptable

Table 29: Risk Appetite

Table30

40	C11	C11: Risk of insider threats and malicious insiders [15] [22]	Confidentiality loss	Modification data can be there	They can make the data unavailable	Really unacceptable
41	C12	C12: Risk of lost of data through migration of data [15]	Confidentiality will also be effected in such case	Modification of data will be there	Unavailability of data will be effected	Really unacceptable
42	C19	C19: Risk of difficult backup procedure [20]	Confidentiality of data is ok	No effect	Its highly effected in such manner	Acceptable
43	C20	C20: Risk of multi tenancy property of cloud [21] [22]	No effect	No effect	No effect	Moderate
44	C22	C22: Risk of repudiation of the information [21]	To some extent	Effect on integrity	No much effected	Moderate
45	C24	C24: Risk of improper key management in backup [22]	Confidentiality will be highly effected	Modification will be less effected	Will be partially effected	Unacceptable
46	C25	C25: Risk related to Data Governance and Compliance [22]	No effect	No effect	No effect	Opportunity
47	C26	C26: Risk in SLA [22]	Not much effect	Not much effect	No much effect	Moderate
48	C28	C28: Risk of compliance and data location [35]	Confidentiality will be effected	No effect	Availability loss can be possible	Acceptable
49	C30	C30: Risk in investigation support and forensic investigation [35]	No effect	No effect	Unavailability will be effected due to unspecified locations	Moderate
50	C32	C32: Risk in unavailability of cloud network [35]	No effect	No effect	This cloud be effective due to downtime of the system	Opportunity
51	C34	C34: Risk in mitigation of cloud service in case of business continuity [35]	No effect	No effect	Due to lack in business continuity it would be there as the unavailability of services	Opportunity
52	B2	B2: Risk of attacks from the devices [71]	Breach of confidentiality can be possible	No much effected	Availability can be effected	Moderate
53	B3	B3: Risk of data Loss [71] [85]	Not effected	Not effected	Availability of data effected	Acceptable
54	B8	B8: Risk of no control on data on personal devices [75]	No effect	No effect	No effect	Opportunity
55	B9	B9: Risk of disclosure of private and personal data due to togetherness of storage of personal and corporation data [75]	Confidentiality loss	Effected	Not applicable	Moderate

Table 30: Risk Appetite

Table31

56	B12	B12: Risk of uncontrolled device and enforcing compliance [80]	To some extent	NA	Not applicable	Opportunity
57	B13	B13: Risk of Unknown IP address [80]	Confidentiality will be effected	Integrity can be effected by unknown person	NA	Moderate
58	B14	B14: Risk of advanced threats [81]	Highly effected	Can disrupted the integrity of the data	With such threats It can harm to the overall availability of the data	Really unacceptable
59	B15	B15: Risk of Insider threats [81]	Can harm to the confidentiality for sack of money and all	Can modify the information and mislead the	NA	Really unacceptable
60	B18	B:18 Risk of no proper security standards for mobile devices [81]	Can harm to the confidential data	NA	NA	Opportunity
61	B21	B21: Risk of no control on users downloads [81]	NA	NA	NA	Opportunity
62	B25	B25: Risk of employee Misuse and abuse [86]	Can disclose the confidential data	Can harm the integrity of data to some extent	NA	Unacceptable
63	B27	B27: Risk of mobile threats [40]	Can cause to the confidentiality of the organisational data	NA	NA	Opportunity
64	SN 1	SN1: Risk of disclosure of private information on the sites [48] [60]	Confidentiality of the organisation can be harmed	Not much effect on the integrity of the companies information	Availability of the private information can be effected to some extent	Unacceptable
65	SN 2	SN2: Risk of malicious third party [48]	NA	NA	NA	Opportunity
66	SN 4	SN4: Risk of gaining access to the secret information of organization CKTECK [49]	Confidentiality can be harmed at higher level	Integrity of the organisation data can be on danger	Hacker can make data can unavailable	Unacceptable
67	SN 6	SN6: Risk of social phishing [50]	Risks can effect to the confidentiality of the data	Integrity can also effect	Can harm to the data and make data unavailable	Really unacceptable
68	SN 7	SN7: Risk of inability to control the information regarding user posts in Social Networking [50]	Confidentiality can be harmed	NA	NA	Opportunity
69	SN 10	SN10: Risk of location tracking from mobile social networking [53]	NA	NA	NA	Opportunity{physical location threats}

Table 31: Risk Appetite

Table32

70	SN 11	SN11: Risk of data manipulation [54] [69]	Applicable	Highly applicable	Can make data unavailable by modifying the data	Acceptable
71	SN 12	SN12: Data retrieving risk [54]	NA	NA	Availability of the data can be harmed by compromising the devices at organisation level	Unacceptable
72	SN 14	SN14: Risk of data misuse and abuse [54]	Can harm the confidential data	Can harm the integrity of data to some extent	NA	Unacceptable
73	SN 15	SN15: Risk of social engineering attacks on CKTECK's secret data [60] [63]	Effect on confidentiality of the data	Also harm to the integrity by gaining control over the secret data	Make data unavailable for other users.	Really unacceptable
74	SN 17	SN17: Other miscellaneous risks [62]	NA	NA	NA	Opportunity
75	C3	C3: Risk of auditing and compliance [11] [21]	NA	NA	NA	Opportunity
76	C6	C6: Risk in Secure socket layer [13]	Can harm confidentiality	Can effect integrity	NA	Opportunity
77	C15	C15: Risk of no standard security specifications and loss of control [18] [21]	NA	NA	NA	Opportunity
78	B19	B19: Risk of no visibility to the end users [81]	NA	NA	NA	Opportunity

Table 32: Risk Appetite

Table33

S.No	Risk No	Name of the Risks	Risk response	Proposed Action
1	C31	Risks of natural disaster	Avoidance	Pre, during and Post plans for BC, DR, Incident handling, backup recovery and hot swapping techniques should be there.
2	C13	Malicious outsiders	Mitigation/ reduce	Strong Authentication, Authorization and encryption mechanisms should be applied.
3	C11	Malicious insiders	Mitigation/ reduce	Strong punishment for the volitation of security policy. Security related training and education should be provided to the employee.
4	C32	Risks of unavailability of cloud network	Share /Transfer	Redundancy of systems and backup devices should be maintained. Internet connection should be maintained by at least two ISPs.
5	C21	Risks of service hijacking in cloud	Mitigation/ reduce	Network monitoring tools should be used for protection from service hijacking.
6	B2	Risks from device attacks	Mitigation/ reduce	Unauthorised device should be block, Manual and automatic methods should be used for checking.(RFID sensors,24*7 Guarded environment.)
7	B1	Risks of loss or stolen devices	Share /Transfer	Backup and recovery schemes should be followed by the organisation.
8	B21	Risks of no control on user downloads	Mitigation/ reduce	Block or restricted contents from the application web links. control should be applied on access systems so that users can't use the unauthenticated contents with Own device. Segregation process can also apply for protects
9	B16	Risks of advanced mobile designed malware	Mitigation/ reduce	Preventive mechanism should be followed. try to educate the employees with advanced risks and threats related to BYOD technologies.
10	B7	Risks of malware migration	Mitigation/ reduce	Use safe connection for connection between personal device and corporate device or it should be restricted. do not connect corporate network from Wi-Fi HOTSPOT. Block Bluetooth and Wi-Fi in organisation.
11	SN2	Risk of Malicious third party.	Mitigation/ reduce	Access control mechanism for third party SLA should be there.
12	SN1	Risks of disclosure of private info on the sites.	Mitigation/ reduce	Social media sites shouldn't be allowed in working hours should be blocked at firewall level.
13	SN13	Cybercrime risk and Cyber threats.	Share /Transfer	Good S/W should be used for devices against any king of attack and copying, Can take help from outsourcing softwares
14	SN5	Risks of getting private conversation of the organisation.	Mitigation/ reduce	Inter conversation monitoring to provide security to the conversation.
15	SN14	Risks of data misuse and abuse	Mitigation/ reduce	Segregation between private and persons data related communications.

Table 33: Risk Response and proposed solutions

B INTERVIEW Ques/Ans With CSO at Verizon Communications, India

Question 1:

Do you have personal cloud network in your organization? If yes then how you provide access of such facility to the individual employee in your organization? Is there any authority?

Answer 1:

We have personal cloud infrastructure to provide access to our employees. Once employees are hired, post completion of their background verification, they are given access to the cloud from where they are further given access to their project based systems. All this is done by approval from HR, and project managers.

Question 2:

Is there any existence of BYOD in your enterprise? What kind of problems you are facing with such technology? List some of those problems. BYOD means bringing your own devices at job place

Answer 2:

We have recently allowed BYOD in our org. We are not facing any challenges since we rolled it out in phases and allowed different and select category of employees carry these devices before allowing it for mass users. The network is secured, monitored, and configured to detect and prevent unauthorized activities.

Question 3:

Due to the emergence of social media, are you allowing your employees to use such technologies in working hours and at which level? Are you facing problems? List those.

Answer 3:

We don't allow access to social media sites in working hours. Such sites are blocked at firewall level. Users are however allowed to use those facilities on their personal mobile phones.

Question 4:

Can you list some of the security mechanisms names which you are applying in your organization for maintaining the information security against cloud, BYOD and Social Media?

Answer 4:

- A) We have completely dedicated cloud network for our org which is not shared with any other org.
- B) We have firewall and dmz created to safeguard our network over internet.
- C) byod devices on which we allow corporate communication, are secured with "good" sw

which segregated personal and official data completely and safeguards official data against any kind of attack and coping.

- D) Social media sites are blocked at firewall level. All firewall logs are monitored to view exceptions.

Question 5:

If there are any kind of security incidents happen in your organization then what types of reporting systems you are using?

Answer 5:

We have internal incident reporting and reaction sites in addition to incidents which are reported via networking tools.

Question 6:

Are employees of your organization familiar with information security policy? Do you provide any security awareness training?

Answer 6:

Yes all employees are aware of info security policies. All new joiners are made to undergo mandatory courses covering all aspects of policies. There are multiple groups at different operational and governance level who are engaged to educated users .

Question 7:

With the use of Cloud, BYOD and Social Media are you facing any kind of organization loss Financial loss, reputation loss, regulatory etc. If yes list some of the impacts.

Answer 7:

Since everything is segregated, secured and protected, we haven't faced any data loss or fin loss.

Question8:

What are the several roles of CISO which helps in maintaining the information security management in your organization.

Answer 8:

Ciso, is responsible for

- a) security of information and Data processed in the org.
- b) Have information security group to manage all exceptions,
- c) Do continuous risk management and ensure sufficient security controls on systems,
- d) Defining and reviewing and cascading security policies to one and all,
- e) Governance, assessment of security health poster in the org via periodic internal audits.

C INTERVIEW Ques/Ans With Senior System Analyst at Corporation Accenture, Oslo, NORWAY

Question 1:

Do you have personal cloud network in your organization? If yes then how you provide access of such facility to the individual employee in your organization? Is there any authority?

Answer 1:

No, our Organization do not have personal cloud network.

Question 2:

Is there any existence of BYOD in your enterprise? What kind of problems you are facing with such technology? List some of those problems. (BYOD means bringing your own devices at job place)

Answer 2:

No, there is no existence of BYOD in our enterprise. No employee is authorized to bring our own devices at workplace.

Question 3:

Due to the emergence of social media, are you allowing your employees to use such technologies in working hours and at which level? Are you facing problems? List those.

Answer 3:

No one is allowed to access social media on company's assets in our enterprise. Accessing Social media like Facebook, Twitter, Orkut leads to security breach, thus access is restricted.

Question 4:

Can you list some of the security mechanisms names which you are applying in your organization for maintaining the information security against cloud, BYOD and Social Media?

Answer 4:

NA

Question 5:

If there are any kind of security incidents happen in your organization then what types of reporting systems you are using?

Answer 5:

Unknown at my designation.

Question 6:

Are employees of your organization familiar with information security policy? Do you provide any security awareness training?

Answer 6:

Yes, they are. Following are information security policies implemented in our enterprise:

- (Data Management) sets out the requirements for the protection of specific Information Assets owned by the Company and those entrusted to it by clients and other third parties.
- (System Security) is a technical Policy that sets out requirements for systems that store and process data, and networks that provide access to data.
- (Acceptable Use of Information, Devices, and Technology) sets out requirements for the way individuals interact with systems and data.
- (External Personnel Access to Company Systems) defines the circumstances under which external personnel can be granted access to Company systems and services.

Security awareness training is provided. Trainings like:

1. Security Awareness and protection
2. Ethics and compliance Training

Question 7:

With the use of Cloud, BYOD and Social Media are you facing any kind of organization loss financial loss, reputation loss, regulatory etc. If yes list some of the impacts.

Answer 7:

NA

D INTERVIEW Ques/Ans With IT Administrator at Corporation Velosi, Oslo, NORWAY

Question 1:

Do you have personal cloud network in your organization? If yes then how you provide access of such facility to the individual employee in your organization? Is there any authority?

Answer 1:

Yes, we have. Each user has his or her own login id and password. All the users are granted permissions according to their designation.

Question 2:

Is there any existence of BYOD in your enterprise? What kind of problems you are facing with such technology? List some of those problems. BYOD means bringing your own devices at job place

Answer 2:

We, use company's laptops and phones for professional use not our personal devices

Question 3:

Due to the emergence of social media, are you allowing your employees to use such technologies in working hours and at which level? Are you facing problems? List those.

Answer 3:

no, it is not allowed.

Question 4:

Can you list some of the security mechanisms names which you are applying in your organization for maintaining the information security against cloud, BYOD and Social Media?

Answer 4:

NA

Question 5:

If there are any kind of security incidents happen in your organization then what types of reporting systems you are using?

Answer 5:

Unknown at my designation.

Question 6:

Are employees of your organization familiar with information security policy? Do you provide any security awareness training?

Answer 6:

Yes, they are. When we join the company, we need to pass e-learning exams which are related to security policies.

Question 7:

With the use of Cloud, BYOD and Social Media are you facing any kind of organization loss Financial loss, reputation loss, regulatory etc. If yes list some of the impacts.

Answer 7:

NA

E INTERVIEW Ques/Ans With System Analyst at TCS Corporation Chicago, USA

Question 1:

Do you have personal cloud network in your organization? If yes then how you provide access of such facility to the individual employee in your organization? Is there any authority?

Answer 1:

No.

Question 2:

Is there any existence of BYOD in your enterprise? What kind of problems you are facing with such technology? List some of those problems. BYOD means bringing your own devices at job place

Answer 2:

Not Allowed, Only Company listed devices.

Question 3:

Due to the emergence of social media, are you allowing your employees to use such technologies in working hours and at which level? Are you facing problems? List those.

Answer 3:

Not allowed to use social media at office Network, Proxy enabled network in use.

Question 4:

Can you list some of the security mechanisms names which you are applying in your organization for maintaining the information security against cloud, BYOD and Social Media?

Answer 4:

No Cloud in use yet.

- Manual checking by Guard for the laptops in carry bags for own devices. USB and other media ports disabled(BYOD-Security).
- Proxy enabled Internet(Social media).

Question 5:

If there are any kind of security incidents happen in your organization then what types of reporting systems you are using?

Answer 5:

Reporting is done to senior manager and based on severity of issue it could lead from a warning to suspension from job at hand and letter from HR to your personal file (which could cause difficulties getting another job).

Question 6:

Are employees of your organization familiar with information security policy? Do you provide any security awareness training?

Answer 6:

Yes the employees are aware and there is an annual mandatory recurrent training .

Question 7:

With the use of Cloud, BYOD and Social Media are you facing any kind of organization loss Financial loss, reputation loss, regulatory etc. If yes list some of the impacts.

Answer 7:

Not aware of any right now, proper measure are taken to ensure nothing like that happens as listed above.

F GLOSSARY

BYOD————- Bring your own device

ISACA————- Information Systems Audit and Control Association

ISO————- International standard organization

CSO ———— Chief security officer.

TCS ————- TATA consultancy services.

PWC———— PricewaterhouseCoopers

SANS———— System Administration, Networking, and Security Institute

HTML———— Hyper text mark-up language

NIST————- National Institute of standards and technology.

Saas ————Software as a service.

Paas————Platform as a service.

Iaas ————Infrastructure as a service.

CRM———— Customer relationship management

Apps———— Applications

APIs————- Application programming Interface.

EC2————- Elastic Compute Cloud

S3————Simple Storage Service

CISCO————- Chief Information security Officers

3G and 4G—- 3 Generation and 4 Generation.

PCs————- Personal computer

IBM————International Business Machines

VPN————Virtual private network.

CIA————- Confidentiality , Integrity, Availability.

AT & T——— American Telephone & Telegraph

BPO———— Business process outsourcing.

RFID————- Radio Frequency Identification

SAP———— System application programming.

ERP————- Enterprise resource planning.

PHP———— Personal home pages.

VC++——— Visual C++

CAD————Computer aided design.

CAME——- Computer Aided Manufacturing Environment

LAN————Local area network

MAN———Metropolitan area network

WAN———Wide area network

WLAN——Wireless local area network.

VDI————-Virtual desktop interfaces.

CFO——— Chief Financial officers

HR————- Human resources.

UNIX——- Uniplexed Information and Computing System

BU————- Business Units.

AAA——— Authorization, Authentication, Accounting

TCG————- Trusted Computing Group

COBIT——- Control objectives for information and related technology.

HTTP———— Hyper text transfer protocol

XML———— Extended mark-up language.

VM————Virtual machines.

SLA———— Service level agreement.

SSL———— Secure socket layer.

Wi-Fi———— Wireless fidelity.

IP————-Internet protocol.

IPS/IDS——Intrusion prevention systems/Intrusion detection systems.

SQL———- Structured query language.

JPEG——— Joint photography expert group.

URL——— Universal resource locator.

CEO——— Chief executive officer.

ROSI———Return on security investment

ROI———Return on investment

NPV———Net present value

DMZ——- Demilitarized Zone.

USB———- Universal serial bus.