PRESENT STATUS OF INFORMATION TECHNOLOGY AND SECURITY MEASURES IN NEPALESE BANKING INDUSTRY

By:
Ajit Regmi
Shanker Dev Campus
Campus Roll No: 2057/061

A THESIS SUBMITTED TO:

Office of the Dean
Faculty of Management
Tribhuvan University
Kathmandu

In Partial fulfillment of the requirement for the degree of

Master of Business Studies (M.B.S.)

Ramshahpath, Kathmandu

February 2009

RECOMMENDATION

This is to certify that the thesis

Submitted by:

Ajit Regmi

Entitled

PRESENT STATUS OF INFORMATION TECHNOLOGY AND SECURITY MEASURES IN NEPALESE BANKING INDUSTRY

has been prepared as approved by this Department in the prescribed format of Faculty of Management Tribhuvan University. This thesis is forwarded for examination.

....
Dr. Geeta Pradhan
Thesis Supervisor, Associate Professor

.... Er. Shankar Adhikari Thesis Supervisor	.... Dr. Kamal Deep Dhakal Campus Chief

VIVA VOCE SHEET

We have conducted the viva –voce examination of the thesis

Presented by

Ajit Regmi

Entitled

PRESENT STATUS OF INFORMATION TECHNOLOGY AND SECURITY MEASURES IN NEPALESE BANKING INDUSTRY

and found the thesis to be the original work of the student and written according to the prescribed format. We recommend the thesis to be accepted as partial fulfillment of the requirement for the degree of

Masters in Business Studies (MBS)

Viva Voce Committee

Head, Research Department:...

Member (Thesis Supervisor):..

Member (Thesis Supervisor): ....

Member (External Expert):..

ACKNOWLEDGEMENT

This thesis has been prepared and submitted to Shaker Dev Campus as a partial fulfillment of the requirements of Masters in Business Studies (MBS) program offered by Tribhuvan University.

With due respect, I express my humble gratitude to my thesis guide Er. Shankar Adhikari and Associate Professor Dr. Geeta Pradhan for their help, guidance and kind of supervision extended to complete this thesis on time.

My next grateful acknowledgement would go to the staff of Nepal Rastra Bank, Kumari Bank, NABIL Bank, Agriculture Development bank, NIC bank and Everest bank for providing all necessary data and required information for this study. Similarly, I would like to thank librarians of Shanker Dev Campus and Tribhuvan University for providing various books, reports, journals and other publications.

I want to express my sincere thanks to my friends for their inspiration, suggestions and insightful comments during the course of my thesis.

I want to express my special thanks to my parents: Mr. Priyadarshan Regmi/Mrs. Sabitra Regmi, brothers/sisters: Sujit Regmi and Ajita Regmi for their valuable help and suggestions.

Finally, I am thankful to all my well wishers who have directly or indirectly contributed to accomplish this study.

Ajit Regmi

DECLARATION

I hereby declare that the work reported in this thesis entitled " *Present Status of Information Technology and Security Measures in Nepalese Banking Industry"* submitted to Shanker Dev Campus, Faculty of Management, Tribhuvan University, Kathmandu, Nepal is my original work done for the partial fulfillment of the requirement for the Masters degree in Business Studies (MBS) under the supervision of Associate Professor Dr. Geeta Pradhan and Er. Shanker Adhikari, of Tribhuvan University, Shanker Dev Campus.

Date:

Ajit Regmi
Researcher
Tribhuvan University
Shanker Dev Campus

CONTENTS

LIST OF FIGURE

LIST OF TABLE

ABBREVIATION

ABBS	Any Branch Banking Service
ATM	Automatic Teller Machine
BFI	Bank and Financial Institution
CBS	Core Banking System
CCTV	Close Circuit Television
CD	Cash Dispenser
CDMA	Code Division Multiple Access
COBIT	Control Objectives for Information and related Technology
CRM	Customer Relationship Management
DAT	Direct Access Tape
DES	Data Encryption Standard
DFD	Data Flow Diagram
DRP	Disaster Recovery Planning
DSL	Digital Subscriber Line
DVD	Digital Versatile Disk
EBANKING	Electronic Banking
EMI	Equal Monthly Installment
GSM	Global Service Mobile
HDD	Hard Disk Drive
HDLC	High Level Data Link Control
HSM	Host Security Management
ICT	Information and Communication Technology
IS	Information System
ISO	the International Standards Organization
IS-MS	Information System Management System
IS-RA	Information System Risk Assessment

IT	Information Technology
LAN	Local Area Network
MIS	Management Information System
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PNB	Panjab National Bank
POS	Point Of Sale
RAID	Redundant Array of Independent Disks)
RAM	Random Access Memory
RDMS	Relational Database Management System
ROM	Read Only Memory
SCT	Smart Choice Technology
SSL	Secured Socket Layer
UPS	Uninterrupted Power Supply
UTP	Untwisted Pair
VPN	Virtual Private Networking
V-SAT	Very Small Aperture Technology
WAN	Wide Area Networking

CHAPTER - I

INTRODUCTION

1.1 Background of the Study

The twentieth century brought huge development in the field of science and technology especially in Information Technology. The fabulous achievements of computer hardware and software over the past few years have changed the way the business operates. Technology has made it easier for consumers to access financial services and cheaper for providers to develop and deliver them. The function of information technology has changed whereby IT has become driving factor instead of supporting factor.

While computer by itself is the most cherished invention that man has ever accomplished, its union with communication technology has brought yet another amazing extension to its already fabulous capabilities. Joining this powerful communication environment, IT has opened flood gates for global economic activity. The modern IT has enough capabilities to enable banks, financial institutions and others to bring about the desired changes

The use of computer and information technology in banking sector has started from the very beginning when they were available for commercial purpose. In the infancy, business computers were used for the practical business of computing the payroll, keeping track of accounts payable and receivable, processing reporting activities at back office and other supporting activities of the bank. As applications were developed that provided managers with information about sales, inventories, and other data that would help in managing the enterprise, the term "MIS" arose to describe these kinds of applications. The definition of MIS varies from authors to authors. Management Information Systems (MIS) is the term given to the discipline focused on the integration of computer systems with the aims and objectives on an organization (*http://www.bestpricecomputers.co.uk*). 'MIS' is a planned system of collecting, processing, storing and disseminating data in the form of information needed to carry out the functions of management.

The development and management of information technology tools assists executives and the general workforce in performing any tasks related to the processing of information. MIS and business systems are especially useful in the collection of business data and the production of reports to be used as tools for decision making. Technology, in all its forms, has had an impact on virtually everyone. Information technology, with its complexity and dramatic change, has arguably had the most profound impact on people.

One can easily remember the days when he/she physically had to go to a bank branch to deposit or withdraw money and get a bank statement book manually updated by a teller over the counter. With the introduction of computer networks, a networked printing machine started replacing the manual update of statements. Phone banking was a revolutionary concept in banking since it made banking accessible virtually from anywhere as long as phones were available. Now cash dispensers (CDs) and automated teller machines (ATMs) are introduced to facilitate withdrawals, deposits and even transfers accommodating mobility in much wider geographical areas. With the successful diffusion of mobile phones, people can easily get their banking services from their mobile phone. Now, one of the most substantial changes in banking technology is the recent introduction of internet banking

The Financial Reforms that were initiated in the early 90s and the globalization and liberalization measures brought in a completely new operating environment to the Banks that were till then operating in a highly protected environment. Services and products like "Anywhere Banking" "Tele-Banking" "Internet banking" "Web Banking" , e-banking, e-commerce, e-business etc. have become the buzzwords of the day and the Banks are trying to cope with the competition by offering innovative and attractively packaged technology-based services to their customers. The networking of the already-computerized branches also assumed urgency and some of the Banks have started inter-connecting their computerized branches using leased telephone lines, Fiber Optic line, radio link or Very Small Aperture Terminals (VSATS). The use of sophisticated banking applications and innovations in networking media in this decade is helping the banks to centralize its entire database in one location. With the introduction of the Internet and the World Wide Web, customer can access and make transactions in their account via internet from home, cybercafé, mobile phones etc.

The use of technology should be well managed and the information should be secured for the success of any institution. There has been tremendous increase in digital information security technology and equipments along with the innovations in Information technology. Along with the use of use of network, banks have started using physical and logical security mechanisms.

The IT journey of Nepal started with the use of computer to process census data in 1971(Baral Ranjan: 2006). There after banking sector has become the technology leader. Agricultural Development Bank Nepal (ADBN) was the first financial institution to introduce Computer technology in Nepalese banking history. Initially computer was used in teller and in back office. The in house developed applications (software) were used mostly to perform those operations. Now information technology is used by all banks. The use of IT is beyond the back office operations, new products such as SMS banking, internet banking, ATM is being lunched by Nepalese banks.

1.2 Focus of the Study

The banking industry has been significantly influenced by evolution of technology. Information Technology has been the driving factor in the banking system rather than previous supporting factor. The information system varies from decentralized system, to centralized and distributed system. The evolution of banking technology has been mainly driven by changes in distribution channels as we see evidence from automated-teller-machine (ATM), tele-banking, pc-banking and most recently internet banking (IB). E-banking products and services are getting more and more advanced and increasing in variety; from providing information at the early stage to providing transactional activities. This study will be focused mainly on different system used by banks.

The introduction of new products by the banks is mostly due to advancement in communication media. Different types of communication media is used for networking. The transmission networks consist of VSAT, microwave radio network, dial up, CDMA, GSM mobile phone and optical fiber network. Due to hilly terrain, Satellite is heavily used where there is difficulty to lay wire line network. These days radio network is also widely used though it has own problems of frequent disturbance, low quality etc. Out of these transmission media, Optic fire is new, more secure and cheap communication media. Each transmission network has merits and demerits. The study will also be focused on those transmission networks, their merits and demerits etc.

Information is one of a financial institution’s most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution. Timely and reliable information is necessary to process transactions and support financial institution and customer decisions. A financial institution’s earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed.

This study will primarily focus on the information security measures adopted by banks. This study will also study Information System used by banks and the networking infrastructure along with their merits and demerits.

1.3 Statement of the problems

The banking industry is experiencing a technological metamorphosis. New technologies such as advanced computer operating systems, wide and local area networks (WAN, LAN), and the Internet, are becoming significant strategic areas for financial institutions. Still, Information and Communication Technology in Nepalese banking sector is at infant stage. Though computerization of banks started before twenty years ago, it was limited to Agricultural Development Bank only. The nation's two largest and oldest banks started using Information Technology only few yeas back. The use of latest technology came only after the establishment of join venture banks. Lack of adequate skilled and experience IT security experts hindering the banks from well secured system which is essential for any financial institution.

IT is central to banking. It has moved from being just a business enabler to being a business driver. Banks are focused on three areas: meet customer's service expectations, cut costs, and manage competition. For this banks are exploring new financial products and service options that would help them grow without losing existing customers and IT has changed the way a bank reaches out to its customers. Gone are the days where IT was deployed for automating accounting/back office functions to remove drudgery of employees; it is now massively being deployed for customer interfacing/interaction." And any new financial product or service that a bank offers will be intrinsically related to technology.

The storage and transmission of information assets in digital form is not only easy and convenient; it is equally vulnerable to unauthorized access and destruction. Every new technology is a target for hackers, crackers, spy ware, Trojans, worms, and malicious viruses. In the early days of the Personal Computer, the worry was viruses. With the advent of the World Wide Web and the exponential expansion of the Internet in the late 1990s, the worry became hackers and denial of service attacks. Now, at the dawn of the new millennium, the worry has become spam, malware/spyware, email worms, and identity theft. All of this begs the question: How do we protect ourselves from this perpetual onslaught of ever-adapting attacks?

In this scenario, this researcher felt the need to study on current Security measurement techniques applied by the banks, since they are the organizations which carries out financial transactions. Then chooses the topic *"Present Status of Information Technology and Security Measures in Nepalese Banking Industry"*

The main problems under which research will be carried out are:

1. What is the status of information technology in Nepalese banking sector?
2. What are the network media currently used and the merits and demerits of them?
3. What does information security actually imply?
4. What are the security measures adopted to safeguard information assets?
5. What are the measures adopted to recover system in case of disaster?
6. What are the weaknesses in present security mechanisms?

1.4 Objective of the study

The acquisition and the treatment of information is a central activity in banking and the impact of innovations in IT is likely to be banking is among the most IT-intensive industries and among those that started earlier to rely massively on computers for their operations. The security of the industry's systems and information is essential to its safety and soundness and to the privacy of customer financial information. Moreover; there have been tremendous growth and diversification in banking activities over the last decade. The specific objectives of the study are to:

1. To examine the existing application of information technology and networking technology in banking industry.
2. To analyze the security measures applied for safekeeping of Information and communication infrastructure and information assets.
3. To evaluate the dependency of banks on information System.
4. To suggest the concerned organization based on findings for reliable and secure information system.

1.5 Significance of the study

This study is concerned with the existing status of Information technology and the security measures applied in Nepalese banking sector. This study explains the current developments of information technology and the theoretical and practical concepts of security methods. This will also identifies the major problems in management of Information security. The output of the study will help to develop Information security and risk management policies in banking sector. All the concerning parties related to information technology and banking will get benefited from it.

It is anticipated that the study actually highlights present weakness in Information security in banking sector. Since only a few researchers have conducted on the related topic and no research is done mainly focusing information security, the study of Information System with focus on Information security of Nepalese financial sector will be a valuable asset for Information Security practitioners, banking professionals, students interested in Information security, Information security policy makers and related government and non-government bodies .

1.6 Limitation of the Study

Like any other thesis, this will also have some limitations as the study also takes data from secondary sources and that data will be assumed valid. The major limitations can be pointed as:

1. The study will be based in Kumari Bank Ltd, NIC Bank Limited, Agriculture Development Bank Ltd., Nabil Bank Ltd and Everest bank limited of Nepalese banking industry.

2. Both primary and secondary data will be utilized in study and to draw conclusions.
3. The study will mostly cover the security measures applied on present day and not the history of what were done before it.

1.7 Organization of the Study

The study has been organized in to five chapters each devoted to some aspects of the study of the Information Technology and Security Measures in Nepalese banking sector.

The chapters one to five consists of introduction, review of literature, research methodology, presentation and analysis of the secondary data and primary data, and summary, conclusions and recommendations. To follow the simple research methodology, it is rational behind this kind of organization of the study as:

Chapter I: it contains the "Introduction" of the study, where it deals with general background, statement of the problems, objective of the study, limitation of the study and organization of the study and other introductory framework.

Chapter II: it consists of "Review of literature". This deals with the review of different literature which are closely related to this study such as review of the related books, journals, articles and the published and unpublished research works as well s thesis. Such review provides a strong base for next chapters.

Chapter III: It describes the "Research Methodology". To find the result of research, some methodology should be followed, which helps to meet the objectives set in the chapter one.

Chapter IV: This focuses on the "Data Presentation and Analysis". This chapter is the major part of the whole study in which all collected relevant data are analyzed and interpreted with the help of different tools. In this chapter major findings of the study will be explained in detail.

Chapter V: This is the last chapter of the thesis. This stated the "Summary, Conclusion and Recommendation".

CHAPTER -II

REVIEW OF LITERATURE

The review of literature is an essential part of all studies. It helps to avoid investigating problems that have already been definitively answered. It is an integral and mandatory process in research works. It is necessary to show how the problem under investigation relates to previous research within theoretical framework and in such situation the underlying theory needs to be reviewed well.

The research has also reviewed related literatures. Firstly, it has reviewed literature for conceptual framework which helps to develop concept about electronic banking and security mechanism and terms related to it. Then important journals, previous master degree thesis, articles and newspapers related to the research topics were reviewed on the second part. It helps the researcher not only to find out the research gap bout also helps to precede this study in a systematic manner.

2.1 Conceptual Review

A. Bank

Bank is "a business establishment, in which money is kept for saving or commercial purpose, or is invested, supplied for loans or exchanged." [The American Heritage® Dictionary of English Language1].

The history of modern commercial banking industry dates back to 1937 A.D in which year Nepal Bank Ltd. was incorporated. Till 1984, financial sector was closed to private sector and foreign investors. HMG/Nepal started to liberalize the financial sector in the first half of the 1980s. But it speeded up this process only in early 1990s. Private sector rushed into the finance industries especially after the restoration of democracy in 1990. Most of the commercial banks came into operation during the decade of 1990s.

B. E-Banking

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM) etc. ATM transactions and telephone transactions are considered e-banking. However, the newest e-banking trend is the internet.

The digitization of transaction (E-banking) can help for the standardization of banking products where by substantial reduction in cost is possible.

Electronic banking increase the banking risks in one hand and it increase transparency and competition in banking services in other hand.

Electronic banking uses computer and electronic technology as a substitute for checks and other paper transactions. It is initiated through devices like cards or codes that let you, or those you authorize, access your account. Many financial institutions use ATM or debit cards and Personal Identification Numbers (PINs) for this purpose. Some use other forms of debit cards such as those that require, at the most, your signature or a scan. E-banking offers the convenience of conducting most of the banking transactions at a time that suits the customer. Customer can access funds and transfer funds between accounts, pay bills and make purchases 24 hours a day, 7 day a week.

E-Banking Delivery Channels in Nepal

i) Telephone banking

Telephone banking is a service provided by a bank and financial institutions which allows its customers to perform transactions over the telephone.

Most telephone banking uses an automated phone answering system with phone keypad response or voice recognition capability. To guarantee security, the customer must first authenticate through a numeric or verbal password or through security questions asked by a live representative. With the obvious exception of cash withdrawals and deposits, it offers virtually all the features of an automated teller machine: account balance information and list of latest transactions, electronic bill payments, funds transfers between a customer's accounts, etc. But currently no fund transfer facility is available in Nepal. Banks which operate mostly or exclusively by telephone are known as phone banks.

Traditionally people can use simple wired phone to directly call the operator of the bank and get some information of the account by revealing their identity. But this service is not available now.

ii) PC Banking

Personal Computer Banking lets the customer to handle many banking transactions via personal computer. For instance, customer may use your computer to view your account balance, request transfers between accounts, and pay bills electronically. For this bank provides the customer a propriety software and customer make connection to the server of the bank using telephone line. With the software provided, customer may take necessary operations on their account. This service was popular before the use of internet for commercial purpose. This service is not available in Nepal. It was never started by Nepalese banks.

iii) SMS Banking

This is the latest e-banking product. In this Customer use their mobile phone's Short Message Service to request the information of banking. Customer can request balance and mini statement of their account or can request cheque book. They can also inquire foreign exchange rate, interest rate etc.

iv) ATM

Automated Teller Machines or 24-hour Tellers are electronic terminals that let you bank almost any time. To withdraw cash, make deposits, or transfer funds between accounts, you generally insert an ATM card and enter your PIN. Some financial institutions and ATM owners charge a fee, particularly to consumers who don’t have accounts with them or on transactions at remote locations.

v) Plastic Card

This is also know as electronic money, e-wallet etc. This typically comes in the form of debit and credit card. Plastic cards are becoming popular because they have following advantages:

- Some businesses—restaurants, for example—don't accept personal checks, but they'll accept credit cards and debit cards;
- Personal checks are rarely accepted outside your city or state, but can use plastic nationally and internationally;
- Using plastic is faster than writing a check;
- You have to remember to reorder checks when you run out;

Generally there are two types of plastic cards.

a) Debit Card

A debit card gives access to the customers' own money. It works like a check because it draws upon your checking account balance. Customers have to have money in the account in order to pay for something with a debit card. Debit Card Purchase Transactions let you make purchases with a debit card, which also may be your ATM card. This could occur at a store or business, on the Internet or online, or by phone.

b) Credit Card

A credit card gives access to a lender's funds. That means a credit card transaction is a type of loan. Every time customers pay for something with their credit card, they are in fact borrowing that amount of money from the credit card company.

vi) Point Of Sale (POS)

Point of sale or point of service (POS or PoS) can mean a retail shop, a checkout counter in a shop, or the location where a transaction occurs. More specifically, point of sale often refers to the hardware and software used for checkouts -- the equivalent of an electronic cash register. Point of sale systems are used in restaurants, hotels, stadiums, and casinos, as well as almost any type of retail establishment. In POS

- Financial transactions are made via Cards.
- Cash is debited from the client's account(s).
- Cash cannot be deposited.

vi) Internet Banking

Internet banking, sometimes called online banking, is an outgrowth of PC banking. Internet banking uses the Internet as the delivery channel by which to conduct banking activity, for example, transferring funds, paying bills, viewing checking and savings account balances, paying mortgages, and purchasing financial instruments and certificates of deposit. An Internet banking customer accesses his or her accounts from a browser— software that runs Internet banking programs resident on the bank's World Wide Web server, not on the user's PC. Net Banker defines a “true Internet bank” as one that provides account balances and some transactional capabilities to retail customers over the World Wide Web. Internet banks are also known as virtual, cyber, net, interactive, or web banks.

Although Internet banks offer many of the same services as do traditional brick-and-mortar Banks, analysts view Internet banking as a means of retaining increasingly sophisticated customers, of developing a new customer base, and of capturing a greater share of depositor assets. A typical Internet bank site specifies the types of transactions offered and provides information about account security. In some cases, web banks are not restricted to conducting transactions within national borders and have the ability to make transactions involving large amounts of assets instantaneously. According to industry analysts, electronic banking provides a variety of attractive possibilities for remote account access, including:

- Availability of inquiry and transaction services around the clock;
- worldwide connectivity;
- Easy access to transaction data, both recent and historical; and
- “Direct customer control of international movement of funds without intermediation of financial institutions in customer’s jurisdiction.”

Levels of Internet Banking

- **Basic information internet-banking/web sites** that just disseminate information on banking products and services offered to bank customers and the general public;
- **Simple transactional internet-banking/web sites** that allow bank customers to submit applications for different services, make queries on their account balances, and submit instructions to the bank, but do no permit any account transfers;
- **Advanced transactional internet-banking/web sites** that allow bank customers to electronically transfer funds to/from their accounts pay bills, and conduct other banking transaction online.

vii) **Any Branch Banking**

Any Branch Banking (ABB) is a facility for bank customers to operate their account from any of networked branches. The branch where the customer maintains his account is the base branch and the branch from where he/she carries out his transactions is referred as the remote branches. Service provided in ABB may differ from bank to bank.

C. Software

Banks use core banking system besides other supporting or surrounding system. The supporting system helps to prepare MIS Reports, Keep record of Human Resource etc. while the core banking system is the main software which is used to operate daily banking activities. Generally banks have following types of software.

a) Core Banking Software

b) Operating System

c) Application software

Types of Banking System

i) Centralized System

Centralization refers to the allocation of all IT resources to one particular business unit that provides IT services to the whole firm (Gordon & Gordon, 2000). The main characteristics of a centralized approach include control, efficiency and economy. Centralized approaches are effective in gaining or regaining control over an organization's information system (Robson, 1997). A centralized IS may have always been centralized or it may be a cost saving regrouping of an organization’s IS to one particular location. The main advantages of centralized systems are that they provide centralized control using established technology and vendors. They thus involve less technical risks. Information Systems professionals providing highly reliable operation maintain such systems. There should be no confusion over responsibilities and the software and hardware used should interface easily (Robson, 1997). Duplication of effort, resources and expertise is also reduced, saving cost and time.

ii) Decentralized System

Decentralization gives individual business units autonomy over their own IT resources without any major considerations over other units unless it is essential to the overall organization policy (Gordon & Gordon, 2000). The main traits of a decentralized approach include flexibility, empowerment of individual business units and service orientation. Decentralized approaches tend to be just as efficient as centralized ones in regard to meeting individual’s needs. In decentralized information systems, startup costs are relatively low (Kroenke & Hatch, 1994). Decentralization also offers benefits of increased accountability, motivation and management responsiveness (Hodgkinson, 1996).

iii) Distributed System

In distributed system a program is split up into parts that run simultaneously on multiple computers communicating over a network. Distributed computing is a form of parallel computing, but parallel computing is most commonly used to describe program parts running simultaneously on multiple processors in the same computer. Both types of processing require dividing a program into parts that can run simultaneously, but distributed programs often must deal with heterogeneous environments, network links of varying latencies, and unpredictable failures in the network or the computers. In distributed banking system, core banking system is processed at branch and centre both. While there is no network connection to the Data Centre, it process locally and when connection resumes, it starts its process from the Data Centre.

D. Hardware

Hardware consists of all the physical equipments that used for electronic activities of the organization. Hardware is a very critical aspect in Information Technology. The performance of hardware determines the performance of the Information technology. The hardware consists of the following types of equipments.

i. Server

Server is the critical hardware of the organization. It has high capacity such as processing power, memory etc. Generally server has different architecture than other workstation. It is built with RISC architecture which is typically having good performance when it is required to process complex and high volume data. They are equipped with more than one processor arranged in parallel mode.

ii. Networking and Security Hardware

a. Hub

A hub is typically the least expensive, least intelligent, and least complicated of the three. Its job is very simple: anything that comes in one port is sent out to the others. That's it. Every computer connected to the hub "sees" everything that every other computer on the hub sees.

b. Switch

A switch does essentially what a hub does but more efficiently. By paying attention to the traffic that comes across it, it can "learn" where particular addresses are. For example, if it sees traffic from machine A coming in on port 2, it now knows that machine A is connected to that port and that traffic to machine A needs to only be sent to that port and not any of the others. The net result of using a switch over a hub is that most of the network traffic only goes where it needs to rather than to every port. On busy networks this can make the network significantly faster.

c. Router

A router is the smartest and most complicated of the bunch. Routers come in all shapes and sizes from the small four-port broadband routers that are very popular right now to the large industrial strength devices that drive the internet itself. A simple way to think of a router is as a computer that can be programmed to understand, possibly manipulate, and route the data being asked to handle. Technically, a wired or wireless router is a Layer 3 gateway, meaning that the wired/wireless router connects networks (as gateways do), and that the router operates at the network layer of the OSI model.

d. Firewall

A firewall is a device that screens incoming network traffic and allows or disallows the traffic based on a set of rules. Firewalls normally sit at the perimeter of an organization's network, protecting it from the Internet, business partners, or other less secure network segments. Firewalls perform screening through packet filtering, through stateful inspection (where the firewall actually looks inside the packet), or through the use of proxies. A firewall is only as effective as its rule base, its configuration, and the people monitoring it. Firewalls must be configured with an appropriate rule set and must be constantly patched to address new emerging vulnerabilities and monitored to detect suspicious activity.

iii. Workstation

Workstation is the computer used by the general user of the organization to do the daily business. Workstation is used to prepare report, print and input the data and to operate the banking software by the staff. Generally PC is used as workstation.

iv. Printer

Printer is a device used to make the hard copy of the report. Printers in large organization such as banks are connected in the network and shared among a large number of users. Printers are of different types such as dot matrix, ink jet and laser. The dot matrix printers are cheaper than other printers. The operating cost of this printer is also low. The main drawback of this type of printer is slow printing speed. Since some banking software cannot print the data in laser and ink jet printer, most of the bank use dot matrix printer.

Another type of printer is ink jet printer. This printer is cheap for purchase but operating cost is very high. Moreover, this printer has slow printing speed.

Laser printer is in high use these days. They print high quality of data. They are costly to purchase but the operating cost of this printer is lower than the ink jet printer. The speed of the laser printer is faster than other type of printer.

E. Communication Network

i.Electronic Communication Environment

a) Leased Line

A leased line connects two locations for private voice and/or data telecommunication service. Not a dedicated cable, a leased line is actually a reserved circuit between two points. Leased lines can span short or long distances. So-called T1 leased lines are common and offer the same data rate as symmetric DSL (1.544 Mbps). T3 lines are a common aggregation of 28 T1 circuits that yields 44.736 Mbps total network bandwidth. Besides being used for long-distance traffic, T3 lines are also often used to build the core of a business network at its headquarters.

b) Optical Fiber

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. These cables are designed for long distance and very high bandwidth (gigabit speed) network communications.

Fiber optic cables carry communication signals using pulses of light. While expensive, these cables are increasingly being used instead of traditional copper cables, because fiber offers more capacity and is less susceptible to electrical interference.

c) V-SAT

VSAT is an abbreviation for a Very Small Aperture Terminal. The transmission rates of VSATs are usually from very low and up to 4 Mbit/s. VSATs' primary job is accessing the satellites in the geosynchronous orbit and relaying data from terminals in earth to other terminals and hubs. The VSAT technology is also used for various types of communications due to its advantages. The main advantage of VSAT is that it can provide wireless communication to anywhere. This is particularly important in Nepal which has hilly terrain and others means of communication is hard to install. The KU band (12-14 GHz) VSAT is widely used. It has drawbacks also. The main drawback is that it gives slow connection due to the latency associated with it. Moreover its speed is also altered by the environment and it is particularly unsuitable in communication of real time application.

d) Radio Link

This technology is a way for transmitting analog and digital signal via microwave radio link. It gives fixed radio connection between two points. This technology has also tremendously used these days. The main drawback of radio link is that it requires line of sight antennas for communication. When some obstacle appeared on the line of the link, it fails to operate.

ii. Network Topology

Network topology is the study of the arrangement or mapping of the elements (links, nodes, etc.) of a network, especially the physical (real) and logical (virtual) interconnections between nodes. Following are the main logical topologies.

a) Bus Topology

Bus networks (not to be confused with the system bus of a computer) use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

b) Ring Topology

In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or device breaks the loop and can take down the entire network.

c) Star and Extended Star Topology

Many home networks use the star topology. A star network features a central connection point called a "hub" that may be a hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.

A type of network topology in which a network that is based upon the physical star topology has one or more repeaters between the central node (the 'hub' of the star) and the peripheral node is extended start topology.

d) Tree Topology

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus and each hub functions as the "root" of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.

e) Mesh Topology

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. A mesh network in which every device connects to every other is called a full mesh.

f) Hybrid Network Topologies

The hybrid topology is a type of network topology that is composed of one or more interconnections of two or more networks that are based upon different physical topologies or a type of network topology that is composed of one or more interconnections of two or more networks that are based upon the same physical topology, but where the physical topology of the network resulting from such an interconnection does not meet the definition of the original physical topology of the interconnected networks.

i. Star-bus

A type of network topology in which the central nodes of one or more individual networks that are based upon the physical star topology are connected together using a common 'bus' network whose physical topology is based upon the physical linear bus topology, the endpoints of the common 'bus' being terminated with the characteristic impedance of the transmission medium where required – e.g., two or more hubs connected to a common backbone with drop cables through the port on the hub that is provided for that purpose (e.g., a properly configured 'uplink' port) would comprise the physical bus portion of the physical star-bus topology, while each of the individual hubs, combined with the individual nodes which are connected to them, would comprise the physical star portion of the physical star-bus topology.

ii. Hierarchical star

A type of network topology that is composed of an interconnection of individual networks that are based upon the physical star topology connected together in a hierarchical fashion to form a more complex network – e.g., a top level central node which is the 'hub' of the top level physical star topology and to which other second level central nodes are attached as the 'spoke' nodes, each of which, in turn, may also become the central nodes of a third level physical star topology.

iii. Hybrid mesh

A type of hybrid physical network topology that is a combination of the physical partially connected topology and one or more other physical topologies the mesh portion of the topology consisting of redundant or alternate connections between some of the nodes in the network – the physical hybrid mesh topology is commonly used in networks which require a high degree of availability..

F. Information Security Methods and Tools

Computer security is the protection of personal or confidential information and/or computer resources from individuals or organizations that would willfully destroy or use said information for malicious purposes. (Timothy Stapko, Practical Embedded Security). One important point often overlooked in computer security is that the security does not need to be limited to simply the protection of resources from malicious sources—it could actually involve protection from the application itself. Building a secure computer system also involves designing a robust application that can deal with internal failures; no level of security is useful if the system crashes and is rendered unusable. A truly secure system is not only safe from external forces, but from internal problems as well. The most important point is to remember that any flaw in a system can be exploited for malicious purposes. Use of cryptography does not guarantee a secure system either; using the strongest cryptography available does not help if someone can simply hack into your machine and steal that data directly from the source. Physical security also needs to be considered. Can a malicious individual gain access to an otherwise protected system by compromising the physical components of the system. Finally, there is the human factor. Social engineering, essentially the profession practiced by con artists, turns out to be a major factor in many computer system security breaches.

i) Physical and Environmental Security

Physical security mechanisms include site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection. Physical security mechanisms protect people, data, equipment, systems, facilities, and a long list of company assets. Information security without proper physical security could be a waste of time. The set for physical security has more to do with physical destruction, intruders, environmental issues, theft, and vandalism. When security professionals look at physical security, they are concerned with how people can physically enter an environment and cause an array of damages. The threats that an organization faces fall into many different categories:

- Natural environmental threats Floods, earthquakes, storms and tornadoes, fires, extreme temperature conditions, and so forth
- Supply system threats Power distribution outages, communications interruptions, and interruption of other natural energy resources such as water, steam, and gas, and so on
- Manmade threats Unauthorized access (both internal and external), explosions, damage by angry employees, employee errors and accidents, vandalism, fraud, theft, and others
- Politically motivated threats Strikes, riots, civil disobedience, terrorist attacks and bombings, and so forth

An organization’s physical security program should address the following goals:

- Crime and disruption prevention through deterrence Fences, security guards, warning signs, and so forth
- Reduction of damage through the use of delaying mechanisms Layers of defenses that slow down the adversary, such as locks, security personnel, barriers
- Crime or disruption detection Smoke detectors, motion detectors, CCTV, and so forth
- Incident assessment Response of security guards to detected incidents and determination of damage level
- Response procedures Fire suppression mechanisms, emergency response processes, law enforcement notification, consultation with outside security professionals

ii) Logical Security

Network Security Tools

a. Firewall

A firewall is a device that screens incoming network traffic and allows or disallows the traffic based on a set of rules. Firewalls normally sit at the perimeter of an organization's network, protecting it from the Internet, business partners, or other less secure network segments. A firewall can run on UNIX, NT, or other operating systems with software that performs packet filtering at a minimum, has been hardened against attack, and has multiple network cards to connect different network segments. Firewalls perform screening through packet filtering, through stateful inspection (where the firewall actually looks inside the packet), or through the use of proxies. A firewall is only as effective as its rule base, its configuration, and the people monitoring it. Firewalls must be configured with an appropriate rule set and must be constantly patched to address new emerging vulnerabilities and monitored to detect suspicious activity. A firewall is like a locked front door. It protects the occupants and contents, but given enough time, an intruder will probably be able to get around the door, either by picking the lock or breaking it down. Such attacks are analogous to attacks against firewalls. Some are more quiet, inconspicuous, and difficult to detect. Others are obvious, and if the occupants take appropriate incident response action, such as calling the police, the attack may stop or be thwarted. However, if the attack is not detected or stopped, the intruder will gain access to the house. Therefore, the firewall needs to be configured correctly and monitored regularly; with appropriate incident response procedures in place should an attack occur. Firewalls should be configured to log all activity. In addition to reviewing the logs for suspicious activity, administrators and the organization can use the logs as forensics evidence in the event of an incident if proper response procedures are followed. The logs should be written to a separate, secure server. If an attacker does obtain unauthorized access to the system, many times the first thing he or she does is to alter the logs. If the logs are written to a secure server, the attacker will have to penetrate it also to get to the logs. Many log review tools can be used to help facilitate reviewing the logs for suspicious activity. These tools look for trends and patterns of activity that could be precursors to attack or actual attacks. The problem with log review is that it is not performed in real time. If suspicious activity is detected, you will know you may have been under attack, but you will not know if you were able to deal with it in time to prevent a successful attack.

b. Virtual Private Networking (VPN)

A VPN can be defined as a private network service delivered over a public network infrastructure. A telephone call between two parties is the simplest example of a virtual private connection over a public telephone network. Two important characteristics of a VPN are that it is virtual and private. The primary reason for deploying a VPN is cost savings. Corporations with offices all over the world often need to interconnect them in order to conduct everyday business. For these connections, they can either use dedicated leased lines that run between the offices or have each site connect locally to a public network, such as the Internet, and form a VPN over the public network.

VPN implementations can be categorized into two distinct groups:

- **Site-to-site VPNs:** Allow organizations to establish VPN tunnels between two or more sites so that they can communicate over a shared medium such as the Internet. Many organizations use IPSec VPN protocols.
- **Remote-access VPNs:** Allow users to work from remote locations such as their homes, hotels, and other premises as if they were directly connected to their corporate network.

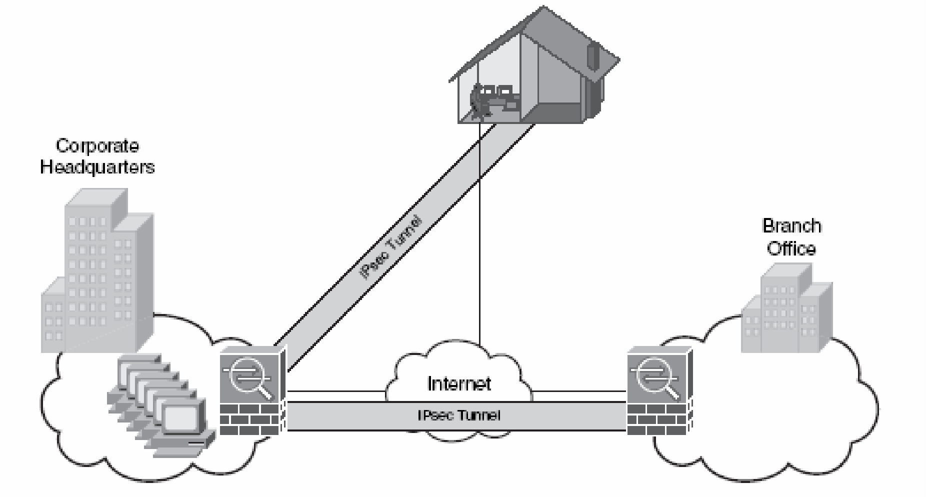


Figure 1 Virtual Private Networking

c. Cryptography (Encryption)

Cryptography is the science of encoding data such that a person or machine cannot easily (or feasibly) derive the encoded information without the knowledge of some secret key, usually a large, difficult to calculate number.

- *Symmetric Key Cryptography*

Symmetric-key cryptography is characterized by the use of a single secret key to encrypt and decrypt secret information. This use of a single key is where the name symmetric came from, the same algorithm and key are used in both directions—hence the entire operation is symmetric. As it turns out, symmetric-key algorithms are the simplest, fastest cryptographic algorithms. The main problem with using the symmetric key approach is finding a way to distribute the key without anyone else finding it out. Anyone who overhears or intercepts the key in transit can later read and modify messages encrypted or authenticated using that key, and can forge new messages. DES, 3DES, and AES are popular symmetric encryption algorithms.

- *Asymmetric Key Cryptography (Public Key Cryptography)*

Public-key algorithms use different keys for both encryption and decryption (hence the asymmetry), and one of these keys is typically referred to as the public-key, since this key is usually published in some public place for anyone to access. The encryption key is called the public key and can be made public. Only the private key, used for decryption, needs to be kept secret. Although the public and private keys are mathematically related, it is not feasible to derive one from the other. Anyone with a recipient's public key can encrypt a message, but the message can only be decrypted with a private key that only the recipient knows. Therefore, a secure communication channel to transmit the secret key is no longer required as in the case of symmetric cryptography.

d. Digital Signature

Encrypting a message with a private key creates a digital signature, which is an electronic means of authentication and provides non-repudiation. Non-repudiation means that the sender will not be able to deny that he or she sent the message. That is, a digital signature attests not only to the contents of a message, but also to the identity of the sender. Because it is usually inefficient to encrypt an actual message for authentication, a document hash known as a message digest is used. The basic idea behind a message digest is to take a variable length message and convert it into a fixed length compressed output called the message digest.

iii) Security Measures:

a. Access Control

Controlling access to information systems and associated networks is necessary for the preservation of their confidentiality, integrity, and availability. Confidentiality assures that the information is not disclosed to unauthorized persons or processes. Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system. The additional access control objectives are reliability and utility. Integrity ensures the Prevention of the modification of information by unauthorized users and Prevention of the unauthorized or unintentional modification of information by authorized users. This is very much important in information security practices. To implement access control, following methods are used.

b. Identification and Authentication

Identification and authentication are the keystones of most access control systems. Identification is the act of a user professing an identity to a system, usually in the form of a logon ID to the system. Identification establishes user accountability for the actions on the system. Authentication is verification that the user's claimed identity is valid, and is usually implemented through a user password at logon time. Authentication is based on the following three factor types:

Type 1: Something you know, such as a personal identification number (PIN) or password

Type 2: Something you have, such as an ATM card or smart card

Type 3: Something you are (physically), such as a fingerprint or retina scan

c. Passwords

Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. This one-time password provides maximum Access Control Systems security because a new password is required for each new logon. A password that is the same for each logon is called a static password. A password that changes with each logon is termed a dynamic password. The changing of passwords can also fall between these two extremes. Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use. Obviously, the more times a password is used, the more chance there is of it being compromised.

d. Antivirus Protection

A virus is a program that requests the operating system of a computer to append it to other programs. In this way the virus propagates to other program. Virus can be easily transmitted such as a file. A virus can be a benign for exampling causing minor disruptions or it might be malignant for example it could delete files, corrupt the other programs so they are unusable or severely disrupts the operations of application systems. Virus can be of three types

- *Virus*

  Virus is a computer program that propagates from one to other computer by attaching with other files. They replicate when certain event occurs.

- *Worms*

Worms are computer program that can propagates with from one to other computer without attaching with other files. They can transmit and replicate in their own.

- *Trojans*

Trojans are malicious computer program that creates the backdoor and transmit the data to other computers.

Organization can implement following types of antivirus controls.

I. Preventive

   a) Check new software with antivirus before its installation.

   b) Check new files with antivirus before they are used.

   c) Download software or files only from reliable source.

   d) Do not use shareware programs that might contain malicious code.

II. Detective

   a) Regularly run antivirus software to detect the infections.

   b) Regularly update the antivirus program with new virus definition.

   c) Check the unexpected modification of the files.

III. Corrective

   a) Ensure clean backup.

   b) Run antivirus program to remove infections.

   c) Have a documented plan for recovery from virus infections.

e. Disaster Recovery Planning (DRP)

DRP which is also called contingency planning involves putting in place the plans to deal with partial or total loss of an organization's information system. The objectives of preparing the DRP are following:

- Ensuring that the data resources of an organization cannot be lost regardless of the nature of a disaster.
- Ensuring that replacement information systems are available as soon as possible to minimize business disruption.

2.2 Review of Articles

Panta Bhubanesh (1992) in his article "*Information Technology and Industrial Sector in Nepal"* has opined that presence of Information Technology and Computer has not guaranteed the improvement in productivity. According to him, this is mainly due to insufficient knowledge about the operation of computer and lack of maximum utilization of the acquired technology. Moreover, another most important cause of this is due to lack of skilled manpower in Nepal. The main problem is not the know how of the installation of the equipment, but the training needs and the depth of the training needs to given to the employee. Another problem is lack of strategy about planning, design and implementation of these technology applications.

Shrestha Prem Shanker(1999) emphasized the "Necessity of Symantec Information System for every organization, industries and offices" to get the right information promptly. He pointed out the function of Information System as follows.

- To get the required information only with specified criteria at time of requirement.
- To keep the information in the database with no duplication i.e. redundancy.
- To update the all the related data at the same time.
- To maintain the integrity of the data.

Simon Mukenge Tshinu and **Gerrit Botha (2005)** in their article " *An integrated ICT Management Framework for Commercial Banking Organizations in South Africa"* tried to find out the framework for managing ICT in banking sector. According to the article Information and Communication Technology (ICT) infrastructure needs to be regarded as the integration of different components that interact with one another directly and indirectly for sustainability of organization's objectives. For the organizations that rely intensely on ICT, such as in the banking industry, it is a necessity to develop practices and tools such as integrated ICT Management Framework that collects best practices found in different ICT Management Frameworks and combine them to business objectives that direct ICT strategies, technologies, and management practices for better management of ICT infrastructure. The main points of their article are:

- There is diversification in the use of ICT Management Frameworks to manage ICT infrastructures in the South African banking industry.
- A minority of organizations operating in the SA banking industry think of the integration of best practices found in different frameworks into a single framework for integrated management of ICT infrastructure.

2.3 Review of Related research studies

Dharshan Shanthamurthy and SS Satchidananda (2004) in their research *"Implementing Information Security at Banks"* have elaborated the prospect of Information Security at Banks. Following is the summary of their study. The application of Information and Communication technology to the banking sector has been growing in the recent past. According to industry estimates, the Bank and Financial Institution (BFI) segment accounts for around 10 percent of the total IT industry. Spending by the BFI segment is expected to jump highly in coming year. The main driver for the increasing use of IT in banking is the need to cater to the growing and changing expectation of the customers who relentlessly demand continuous improvement in the quality of services offered, reduction in charges and access to new products. In the context of global competition, the banks have to use other factors facilitating for the increasing IT investments in banks are the statutory requirement from the Centre Vigilance Commission that banks should achieve 100% branch computerization, availability of certification services for ensuring security of electronic transactions and the growing size, complexity and integrity of the financial markets. Technological advancements bring along concerns on the privacy, confidentiality and integrity of information. It is being seen that such concerns have a major impact on the functioning and existence of banks and financial institutions. While many banks have taken steps to improve their Information Security, much can be done to improve them further. It is often perceived by the management of banks that Information Security is technical and complex. The fact on the contrary is that Information Security is just like any other area of managerial decision. Further, IS investment should also have a return on investment. This is to be achieved by an effective Information Security Risk Assessment. Currently the IS implementation in banks suffers from deficiencies such as:

- A comprehensive Security Risk Assessment is not being conducted before drafting a security policy for the bank.
- The acceptable usage policy (AUP) is not communicated to all staff of the bank.
- The scope of information systems audit at branches is restricted to checklist audits.
- Defined Vulnerability assessment policy has not been set out for the data centers of banks.

Further, IS like any other practice has certain best practices to be followed. Best Practices would not only confine to technical configurations and settings but policy and procedures as well. For banks to make sure that Information Security is properly addressed there is a need to lay out a clear methodology for tackling it.

According to them, following are the important aspects of IS relevant to banks and financial institutions.

- Information Security is not only the concern of the Information Technology Department but for the entire organization. It is said that “Security in an organization is as strong as its weakest link”. Hence each and every user of information, right from the senior management to the clerk in the branch have to be involved in any security initiative taken by the bank. This will mean that they have to be aware of the security threats and should practice the laid down policies and procedures.

- Information Security Policy has to be aligned to the business objectives by a proper information security risk assessment (IS-RA). This means that the risks identified and measured during structured IS-RA should be mitigated with effective security policy and procedures.
- Information Security Policy cannot be the same for all banks despite there being similarities in their business function. This is due to the reason that each bank has its unique risks which might be multidimensional considering their locations, their services, their business goals and their technical infrastructure.
- The Banks can optimize their resource spending in Information Security by strategizing their security spending to mitigate their high impact risks identified during there IS-RA. Hence, Information Security should be seen as an investment.
- Security Audits at branches need to be conducted by qualified personnel as it needs to encompass audit through the computer.
- Information Security consists of Confidentiality, Integrity and Availability of data. Hence in every decision, the security requirement of Confidentiality or Integrity over availability and vice versa has to be evaluated.
- Information Security includes both electronic and paper information.
- Information Security Risk Assessment is not only restricted to vulnerability assessment of technical infrastructure but extends to identifying critical assets, their threats and organizational vulnerabilities. It also includes business impact analysis and measuring risks and suggesting appropriate controls

Bhattarai A.P. (2003) carried out the study on "*Performance of MIS at Kumari Bank*". He carried out the study with the following objectives.

- To identify the factors affecting the performance of the MIS of the bank.
- To examine the existing expertise and situation of software personnel at the bank.
- To study the training provided to the end users regarding the software and security and its effects on the performance of the employee and the software.

The research was conducted based on both primary and secondary data. Observation, questionnaire and direct communication were used to collect the primary data. Data collected from primary sources are displayed in tabular format and data have been analyzed using percentage method. Table and figures, Data Flow Diagram and Flow Chart are used for data presentation.

Bhattarai concluded that Bank has installed latest banking software to meet their information needs. However, the update and support of the software is always needed which becomes costly as the bank does not have expertise to update and support the software. According to him the management of the organization should always be acutely be aware of various factors which affect the performance of the MIS and take corrective actions promptly. He further said various factors such as training to software personnel, training to the operating staffs, good communication link have the direct link to the performance of the software.

He has been successful in accomplishing his specified objectives. However; he has not gone through the security and access control methods in MIS of the organization.

Anu Sunil (2005) conducted thesis on *Information System of C-MODE Inc.* He defined MIS as a traditional term in the organization and states that only computerized MIS is a new method in the organization. He has conducted his study with the following objectives.

- To study the existing information system in the C-Mode incorporation and its co-company www.nepbiz.com.
- To evaluate the efficiency of Information System in the organization.
- To identify the problems and to access the impact of computer information system.

His thesis was mostly based on primary data. He has used personal investigation through investigation. His main source of data is www.c-mode.biz and www.nmepbiz.com. He has also used secondary source of data from brochures of the organization. He found the following drawbacks in the system.

- Case of double charge for customer credit card.
- Errors in the system after modification.
- Lack of laws and regulations in electronic payment system.

The man flaw found in his thesis is that, he reviewed the other thesis on general only. He did not review any thesis in detail even though it was relevant to his study. Still his has gained success in getting his objectives.

Khadka Ashis (2004) has conducted thesis on title *MIS and its application in HMG/DANIDA.* The study mainly focuses on Management Information System of HMG/DANIDA – NARMSAP. The system handles the entire database and provides the information in the form of report to the end users helping in variety of decision making process. He has conducted his study based on following objectives.

- To examine the present Management Information System in HMG/DANIDA.
- To examine the effectiveness of MIS and
- To identify the importance of computerized MIS in the organization.

His research was based on primary data collected from different computer operation manuals, websites and questionnaire. He has presented his data by using tables, figures and flow charts. The major findings of the study was

- HMG/DANIDA is not fully computerized and both manual and computerization was implemented.
- Mostly computer was used for statistical analysis, clerical work, information forecasting and decision making.
- Almost all departments are dependent on computer information system.

Mr. Khadka is successful in achieving the objectives mentioned in the thesis. However he has not given strong recommendation for HMG/DANIDA that might be helpful for the improvement of the information system.

Acharya I. (2002) conducted thesis on *Implementation of MIS at RNAC- A case study in marketing department* with the following objectives.

- To examine the existing Information System of Marketing Department of RNAC.
- To examine the flow and communication of Information among different division and units of marketing department.

The research was carried out using following methodology.

Data was collected from both primary and secondary sources. Observation, questionnaire and interview were the tools used to collect data from primary sources while operating manuals, journals and news letter were the secondary sources of data. Tables and figures, Data Flow Diagram and Flow chart were used to present data. Data collected from primary sources are displayed in tabular format and analyzed using DFD and Flow chart.

He observed the following problems in his study.

- Complex organizational structure and its multi division is making ambiguity in the operation.
- Information System work only in stand alone system, thus they need information system that works in network environment.
- There is insufficient Information Technology Infrastructure.

Though the researcher is successful in achieving his objectives, he has overlooked the study of human resource expertise for management information system.

Raghuvanshi Keshab (2006) conducted the thesis on *MIS in cable Television Organization.* His study was mainly focused on subscriber information system as information of subscriber is vital in service based organization like Cable Television. His main objectives of the study were:

- To examine the performance of Subscriber Information System (SIS).
- To examine the hardware and software environment of SIS.
- To develop effective Decision Support System module.
- To provide recommendation based on findings.

Mr. Raghuvanshi found some limitation of Information management within the organization. Firstly he found that the modification of the system is rarely done. Secondly, there is lack of training program for the users to handle and operate the system and thirdly, there is under utilization of the information system capabilities.

The major drawback this researcher found in his research report is that he did not analyze the questionnaire given to the end users. But he is successful in accomplishing his objectives.

Shrestha Raja Ram (2006) conducted thesis on *MIS in Benchmark Pvt.Ltd. (A Case study of Computer Maintenance Information System)*. He has conducted his research with the following objectives.

- To examine the current Information System for Computer Maintenance Information System.
- To examine the software, hardware and networking environment of the system.
- To evaluate the performance of the Information System.

Mr. Shrestha has used both primary and secondary sources for data collection. Data from primary sources are collected from scheduled interview, observation and questionnaire methods. Secondary data are collected from published reports, brochures, manuals, organizations websites and other logs and forms.

The collected data are presented using tables and figures, flowchart, E-R Diagram and Decision tables.

Mr. Shrestha concluded that the information system used by the organization is appropriate for them. It has become main factor for bringing changes in department and is found effective. It is helping the organization increase productivity. The system has good user interface and is found user friendly.

Mr. Shrestha is successful in achieving his objectives partially. He could not achieve hardware and networking infrastructure that was stated in his objectives of the study.

2.4 Research Gap

The use of information technology in banking sector has changed from supporting factor to driving factor. Now a day banks are lunching their products based on information technology and without IT, the growth of banking sector is hard to imagine. In Nepal also almost all the banks have adopted technology for their growth. Even the traditional banks have started investing in Information Technology. The use of information technology not only provides key competitive advantages, it can also jeopardize the success and sustainability of the organization if not properly managed. Financial sector have started electronic banking whereby customers can make transactions of their account without visiting the brick and mortal institution. They have started using internet banking, SMS banking and Debit and Credit card operations. With these the security has become prime concern for each bank. But there has been very limited research conducted about this in Nepal. We can hardly get any research regarding the use of Technology in Banking sector and the security measures taken by them for secure banking. Hence this research is entirely distinct in the sense of presenting primary as well as secondary data. This research will give concise figures as most data is collected from the primary source.

CHAPTER - III

RESEARCH METHODOLOGY

In this chapter, the methodology used for collecting and analyzing data will be discussed. Every research study can reach towards the proper conclusions adopting the proper methodology regarding the subject matter of study. A research study can produce the fruitful results if an appropriate methodology is taken under consideration to highlight and evaluate the different aspect of the study. Being a novice researcher, it should be kept under considerations that the wings of methodology should not be misdirected. The methodology should be adopted in such a way that the leakages and errors of the study could be minimized. Thus, the quality of the study depends upon the methodology used by researcher.

3.1 Research Design

Any research work cannot be done without the collection of required information. Those required information are generally collected from different resources. A research design is the specification of methods and procedures for acquiring the information needed. The researcher has designed the research based on following facts.

- A plan that specifies the sources and types of information relevant to the research question.
- A strategy specifying which approach will be used for gathering and analyzing the data.
- Both time and cost budget.

The research design is basically focuses on

- Sample Design
- Observation design
- Statistical design

Sampling design deals with the method of selecting the subjects to be observed in a given study. Observation design relates to the conditions under which observation are to be made. Statistical design deals with the question or how many subjects are to be observed and how many are to be analyzed.

3.1.1 Population size and sampling procedure

There are twenty-four commercial banks (www.nrb.org.np) as on Ashad 2065. operating in Nepal at present. Sampling is the process of selecting the sample from the given population. The method of selecting a sample usually depends upon the nature of the investigation. On this research, the researcher has sampled based on judgmental sampling has been used which is based on market perception about good, average and poor Information Technology adopted banks.

3.2 Sources of Data

Both primary and secondary data is used for data analysis and investigation of this thesis. As this type of research has not been conducted before, primarily the primary source of data is used in this research.

3.2.1 Primary Data

Primary data has been collected from different sources. But the primary source is the Nepalese commercial banks that came under the researcher's thesis sample. This type of data includes the data collected by direct interview, formal and information interview with related personalities or information discussion with the staff of the concerned organization. Some of the methods used by this researcher to collect primary data are as follows.

a) Interview

This researcher has conducted interview with key personalities of the Information Technology Department of the sampled commercial banks. They were primarily Head of Department, Security officer and other supporting staff the department. Such interview was very much fruitful to make clear some misunderstanding and technical details followed by the organization.

b) Observation

Some of the data was collected by direct observation of information technology department. This researcher has observed the architecture of the data centre, location of the networking hardware etc. The observation was fair and without prejudice as far as possible.

c) Questionnaire

To collect the precise technical data, questionnaire method was used. The questionnaire was submitted to the head and deputy head of IT department, information Security officer and the technical assistant. (*See Appendix II for Questionnaire Sample*)

3.2.2 Secondary Data

Secondary data was collected by reviewing the policy, documentation, Information Technology strategy and Plan, the security manual etc that were available in hard copy and soft copy form, computer data bank, data services etc. The sources of data and information are:

- Organization's brochures, manuals, organization's website etc.
- Organization's office record concerned with computer maintenance.
- Organization's official forms such as maintenance record form, monitoring and evaluation forms etc.
- organizations' transaction records and log books
- e-banking application forms
- e-banking security manuals
- security manuals provided by hardware and software vendors
- Information Security Policy of the organization.
- Websites of the hardware and software suppliers etc.

3.3 Analytical tools and techniques

With reference to the research methodology, different tools and techniques have been used to present and analyze the existing system. Since the research is descriptive and declarative type, to present the survey findings comprehensively, this researcher has primarily used tables and charts. to make the system more understandable this researcher has used flow chart and data flow diagram(DFD). Following are the brief descriptions of the tools used in this research.

3.3.1 Tables and figures

A table is presentation of data in column and row form. Typically table is used to present data and information more clearly.

3.3.2 Data Flow Diagram (DFD)

DFD is a graphical tool that is used to show how data moves and get transformed in an information system in top-down fashion. It is a logical model or essential model of an information system in a simple, direct way. DFDs are most appropriately used for analyzing business information system because these systems are predominantly data driven. DFDs are not used to show the logics of the program or any detailed processing.

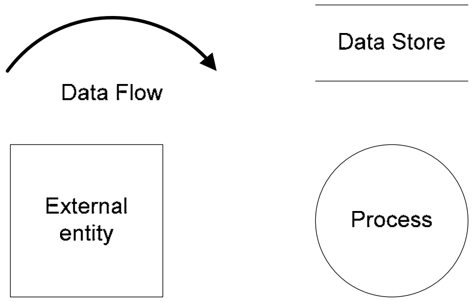


Figure 2. DFD Symbols (Yourdon)

Process Symbol: A circle or bubble; A process modifies or changes data from one form to another. Details of process are not shown in the DFD. The details are documented in description.

Data Flow Symbol:

A line with arrowhead in the direction of the flow; Data flow is the pathway by which data moves from one part of the IS to another part.

Data Store Symbol

Two horizontally parallel lines; Data source is the repository. we use data store in a DFD when we must store the data so that it can be used by some other process. A data store must be connected to a data flow with a process at the other end of the process.

External Entity Symbol

A rectangle symbol; It is a person, department, outside organization, or other information system that provides data to the system or receives data from the system. External entities are also called terminators. An external entity that supply the data is called origin or source and that receives data is called destination or sink.

Level of DFD

Context Diagram or 0 Levels DFD

The first set of DFD of a system is context diagram. It shows data flow between the system and the external entities. Thus, it shows the boundaries of the system and gives top –level view of the system. In this diagram only one process is used to represent entire system and there will be no data store in it.

Lower Level Diagrams

The lower level diagrams shows more detailed data flow of the system. A single process of the Context diagram is exploded to sub process and shows the data flow in detail. To say it in other words, in First level explosion of the process 0, the process 0 is expanded or exploded or decomposed in other major sub process. We include all the entities and data flows that appeal in the context diagram of the system.

3.3.3 Flow Chart

A flowchart is a diagrammatic representation that illustrates the sequence of operations to be performed to get the solution of a problem. Flowcharts are generally drawn in the early state of formulating computer solutions. Flowchart facilitates communication between programmers and business people. These flowcharts play a vital role in the programming of a problem and are quite helpful in understanding the logic of complicated and lengthy problems. Once the flowchart is drawn, it becomes easy to write the program in any high level language. often we see how flowcharts are helping in explaining the programs to others. Hence, it is correct to say that a flowchart is a must for the better documentation of a

Complex program.

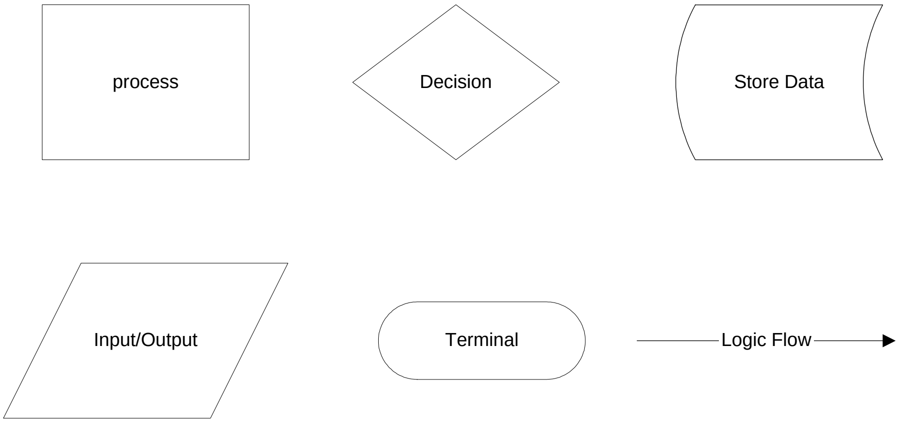


Figure 3. Flowchart Symbols

Terminal: The terminal symbol is used to indicate beginning (START) or ending (STOP) in the program logic flow. It is the first symbol and the last symbol in the program logic.

Processing: A process symbol is used to represent arithmetic, manipulation and data movement instructions. The logical process of moving data from one location of the main memory to another is also denoted by this symbol. When more than one instruction is to be executed consecutively, they are normally placed in a single processing box and they are assumed to be executed in the order of their appearance.

Decision: The decision symbol is used in a flowchart to indicate a point at which a decision has be made and a branch to one or more alternatives points is possible. The criteria for making decision should be clearly indicated within the decision box. Moreover; the condition upon which each of the possible exit paths will be executed should be identified and all possible paths should be accounted for. During execution, appropriate path is followed depending upon the result of the decision.

Input/Output: The input/output symbol is used to denote any function of an input/output device in the program.

Flow lines: Flow lines with arrowheads are used to indicate flow of operation. Hence, flow lines indicate the exact sequence in which the instructions are to be executed. The normal flow of flowchart is from top to bottom and from left to right. Flow lines should not cross each other and such intersection should be avoided whenever possible.

CHAPTER - IV

DATA PRESENTATION, SYSTEM ANALYSIS AND DESIGN

System analysis is a detailed study of the various operations performed by a system and their relationships within and outside of the system. During system analysis, data collected from different sources and methods are studies. After analysis, the most creative and challenging phase of the system life cycle is system design. The term design describes the final system and the process by which it is developed. It provides the technical specifications that will be applied in implementing the candidate system. The developed system is presented using different tools such as Data Flow Diagram (DFD), Flowchart, tables etc.

4.1 Existing Structure of Organization

This part presents the present structure of the information technology division of the organization.

4.1.1 Organization structure

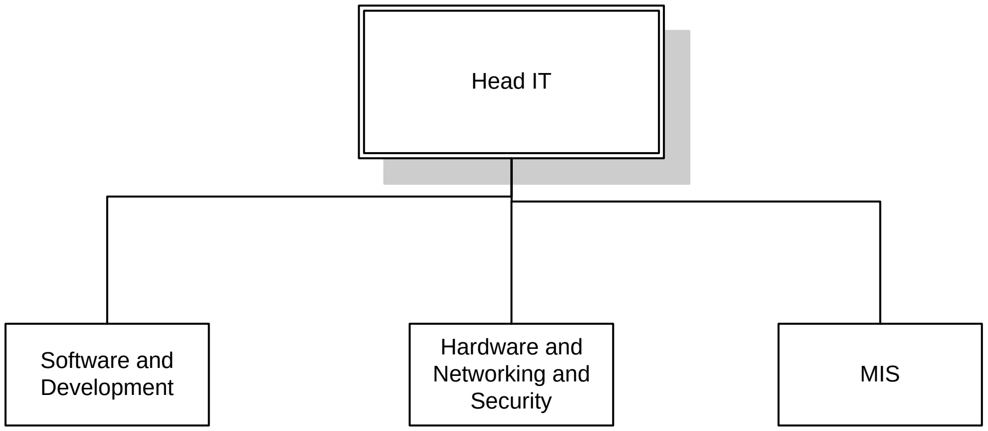


Figure 4 Typical Organization Structure of IT Department

The typical organization chart of Information technology department is shown in the figure above. This shows that IT department is headed by Manager IT and in some bank it is headed by Chief IT department. Though their functional title is Manager IT, they are generally senior Officer or Assistant Manger of the bank. Then the department divides the job as a software unit, hardware and networking unit and MIS unit. The software unit's job is to support all the software that is in use in the bank. The main software is the core banking solution which is used to automate the core banking operation.

The job of hardware and networking unit is to handle entire job related to hardware in use. They are generally Servers, PC, printers and networking equipments. They also troubleshoot the problems associated with the communication link failure. Arranging back up link, handling communication contract etc are the job Networking and Hardware unit.

The job of MIS unit is preparing all the reports required for the bank and regulatory body.

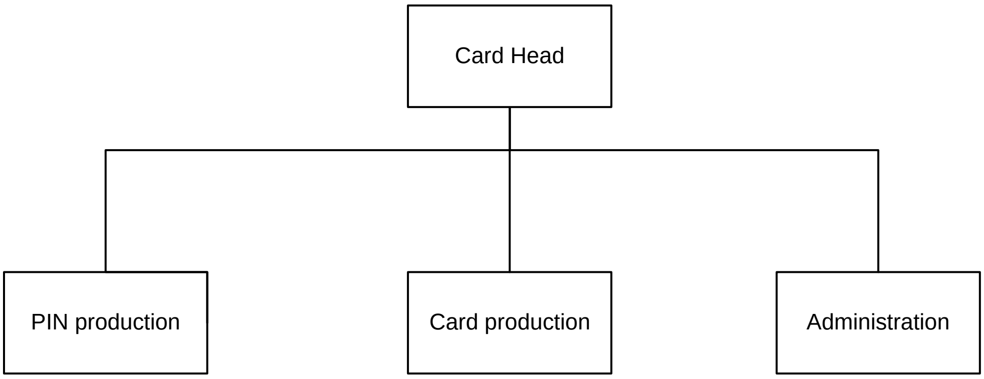


Figure 5 Typical Organization Chart of Card Department

From the data collected it shows that there is no provision for special security administrator. All the end users and expected to cooperate for security for the system and all IT staff have general idea about the security of the system. Due to lack of specialized person, the IT security of the banking organizations are seems not satisfactory.

4.1.2. Designation and Responsibility of personnel

S.N	Designation	Responsibility
1.	IT Head	• overall responsibilities of IT activities, including IT strategy and planning • Responsible for running IT department. • Formulating corporate IT strategy and long term IT planning. • Recommend the Line manager about status, maintenance and upgrade required. • Maintain highest quality standards for providing IT services. • Manage and develop professional training for IT staff. • Monitor day to day IT activities and irregularities if any.
2	Hardware, networking and security Unit	• Implement, support and troubleshoot hardware, including servers, PCs and networking equipment. • Arrange primary and backup networking link. • Communicate with vendor to provide necessary hardware and networking media.

		• Recommend Head IT about the new hardware advancements. • Study and recommend network security devices and technologies. • Setup Virtual Private Networking.
3.	Software and development Unit	• Develop and support small in-software. • Provide primary level support of Core Banking Software. • Communicate with the software vendor regarding the problems and bugs raised in the banking system. • Provide training of operating software to general staff. • Setup necessary parameters in the banking software. • Operate RDBMS of the banking software. • Other Software related issues.
4.	MIS Unit	• Develop necessary software according to the requirements of the management, auditors and regulator. • Prepare and submit MIS report to the concerned units. • Prepare all monthly, quarterly, half yearly and yearly reports.

		- Ensure that MIS is accurate and operational according to the needs of the bank.

Table 1. Duties and Responsibilities of personnel

4.2 Sources of information

The information presentations in this report are obtained primarily from the sampled banks by questionnaire method. More data are collected from the manuals, brochures, security guidelines and policies of the banks. Some information was obtained from the website of the banks. The DFDs of the present system is obtained from the system documentations of the sampled banks and via internet.

4.3 DFD of Present System

4.3.1 Context Level DFD

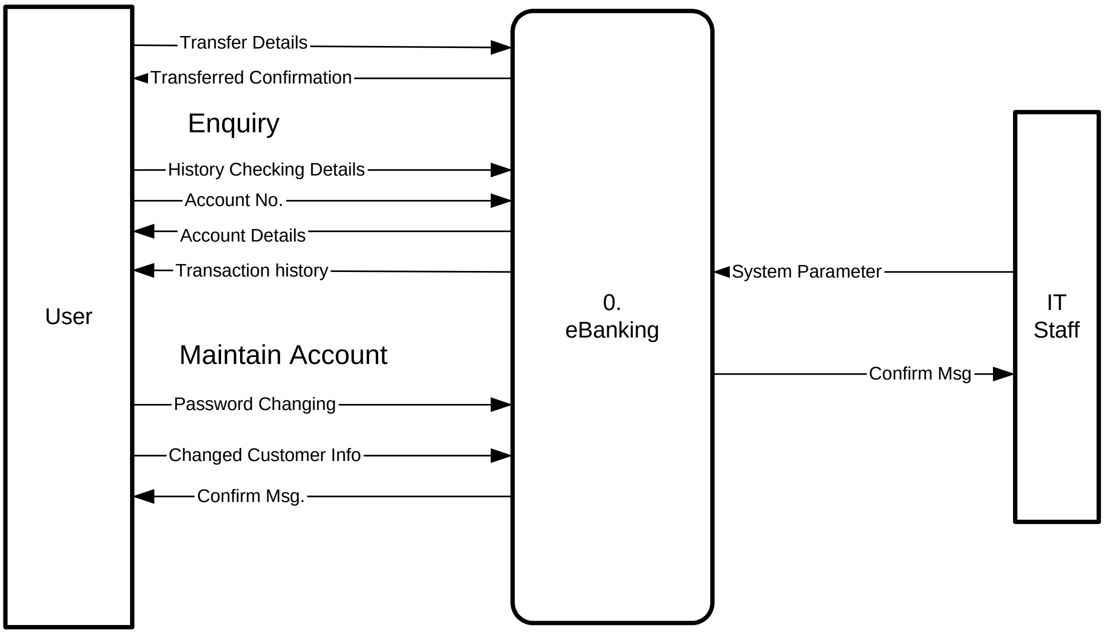


Figure 6 Context Level Diagram

4.3.2 System Level DFD

a) Fund Transfer Module

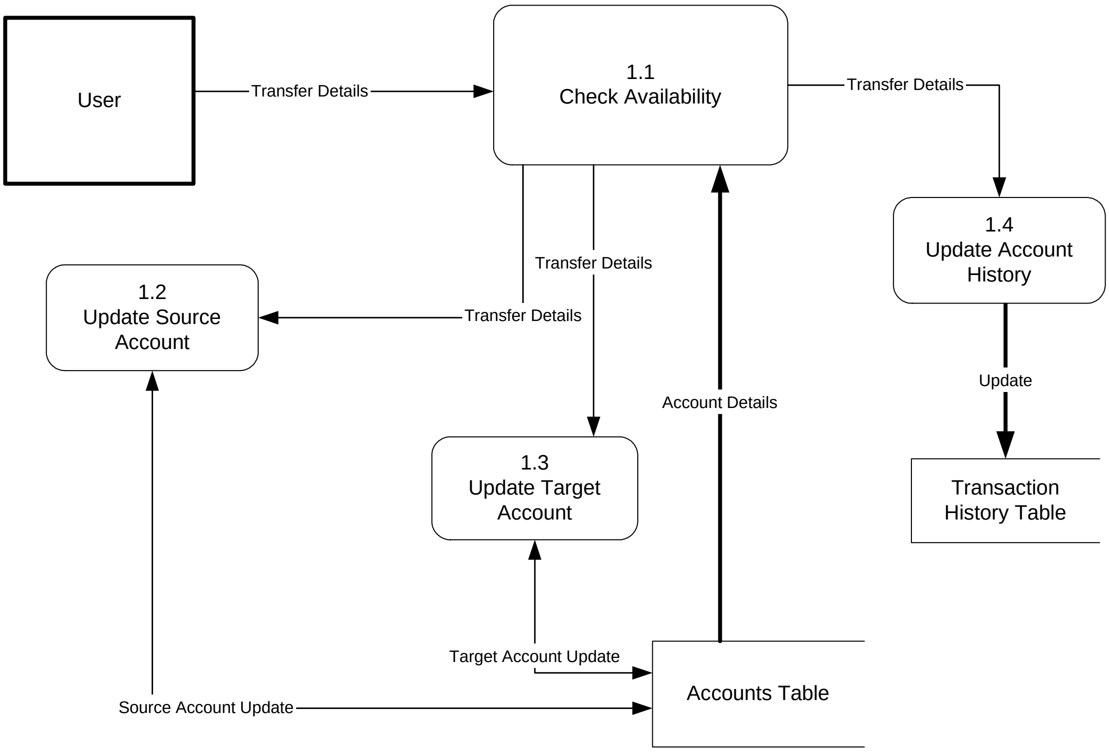


Figure 7 System Level DFD - Fund Transfer Module

Process Name	**Process Description**
Check Availability	To check the availability of the source account for the transfer
Update Source Account	Update the new balance of Source Account
Update Target Account	Update the new balance of Target Account
Update Account History	Update History of the Source Account

Table 2 **System Level DFD - Fund Transfer Module**

b) Inquiry Module

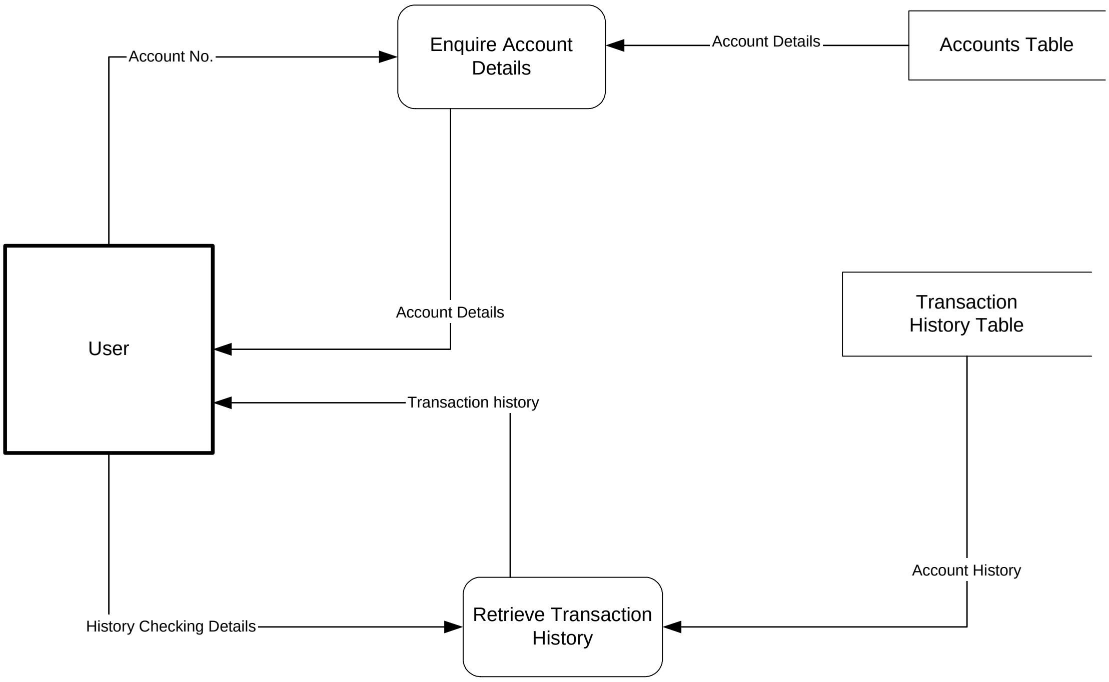


Figure 8 Inquiry Module

Process Name	**Process Description**
Enquire Account Details	Get Account Details for the user.
Retrieve Transaction History	Check Account transaction history

Table 3 Inquiry Module

c) Maintain Account

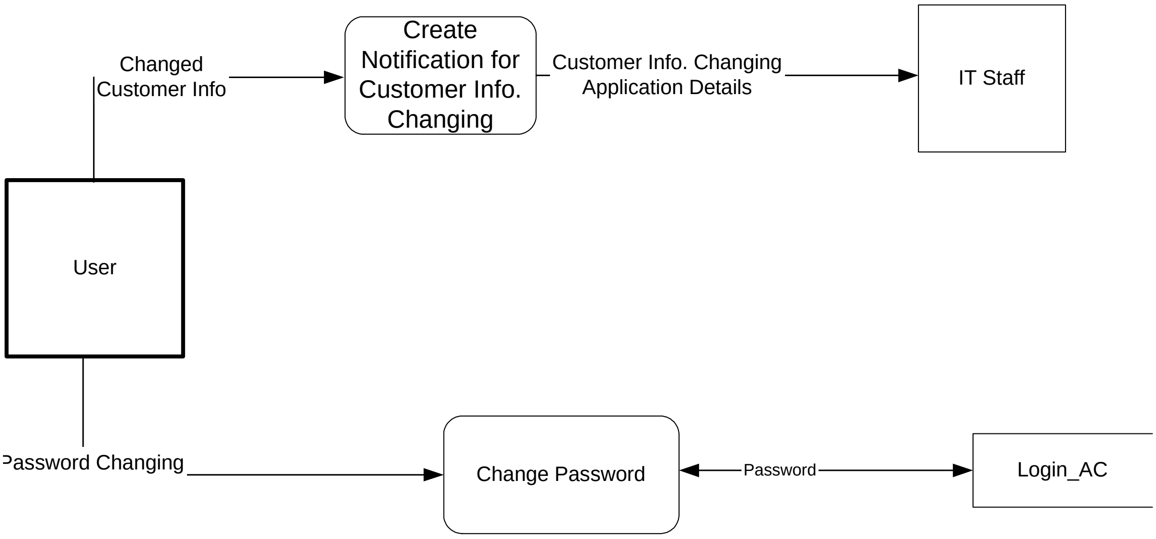

Changed Customer Info
Create Notification for Customer Info. Changing
Customer Info. Changing Application Details
IT Staff
User
Password Changing
Change Password
Password
Login_AC

Figure 9 Maintain Account

Process Name	**Process Description**
Create Notification for Customer Info. Changing	A notification of Customer Info. Changing is sent to a IT Staff
Change Password	Changing user login password for Internet Banking

Table 4 Maintain Account

4.4 Analysis of existing technology

4.4.1 Banking System

Out of the five banks under the sample, three have set up centralized system, and two have installed decentralized system. Those who have decentralized system are not satisfied with the system. With decentralized system, they found providing latest electronic banking products and system support is very hard to manage. Most of them who have decentralized system want to move to centralized system and some wants to move to distributed system. Distributed system is more sophisticated system and with this architecture, banks can continue their operation in the branches even if the communication link to the data centre is down. This is particularly found suitable in Nepal where the quality of network link is not satisfactory in remote areas.

S.N.	System Architecture	Drawbacks
1	Centralized System	• One point failure at the centre stops all the operations of the bank. • If the link to the server goes down, branch cannot operate. • The back up communication link is essential. • Even the small problems cannot be solved at the branches since there will be no staff of IT.
2	Decentralized System	• IT staff is necessary at each branch resulting high cost. • Large no of server is necessary as each branch will have primary and back up server. • Keeping expert IT staff at each branch is

		impossible. • Problems should be handled by IT staff that generally stays at head office, so it takes some time to resume operation. • Providing latest electronic banking services like Any Branch Banking Service, ATM, Debit Card, Internet Banking etc. becomes hard to manage. • Each branch requires license copy of Core banking software and database software which costs higher.
3.	Distributed System	• Complex technology • Data may not be replicated on both places due to connection problems and results in data mismatch. • More costly technology.

Table 5 Banking System

4.4.2 Software Used

S.N.	Type	Name
1	Operating System	• Ms. Windows 2000 Server • Ms. Windows NT Server • Ms. Windows 2003 Advance Server • Sun Solaris • Linux • IBM AIX
2	Core Banking System (CBS)	• Globus • Finacle • Pumari • In house developed – no specific name.
2.	Database	• Ms. SQL Server • Oracle 8i and above • Jbase
3.	Application on CBS	• Internet Banking • Telebanking • SMS Banking • Deposit Module • Loan Processing Module • Asset Liability Management

Table 6 Software Used

It is found that none of the banks have 100% automated System. Most of the banks have more than 75% of the system is automated.

The software used for security is similar in all the banks. All banks have installed firewall, antivirus, anti ad ware and anti spy ware software.

4.4.3 Hardware in Use

S.N	Type	Configuration
1.	Server Brand: IBM, HP, Dell	• 4 Processors • 4 to 32 GB RAM • 40 – 146 GB HDD (Generally more than 1) • DVD ROM • External DAT drive. • 4Gbps RAID Controller
2.	Network Hardware	• Router • SWITCH • HUB • Modem
3	Security Hardware	• Firewall o Cisco PIX o Cisco ASA

		o Fort iGATE o Firebox • HSM • Router
4	PC as a server	• Pentium 3 and above • more than 1Ghrz processor • more than 40 GB HDD • more than 512 MB RAM • DVD R/W

Table 7 Hardware in Use

4.4.4 Network Technology

Most of the banks have employed extended start network topology. Banks have rarely employed mesh technology. Mesh technology is implemented to keep the redundant link to the branch. This helps the branch to resume the connection to the server when the primary network link fails. This is used by the banks which have not separately installed the back up link to the server.

It is found that most of the organizations have employed Optic fiber technology to connect to the branches. Some have implemented V-SAT technology. This is used mostly in the remote branches where the other means of communication link does not exist. Due to high cost, this technology is being replaced by the bank as soon as the other means of communication becomes available.

Some banks have used radio link, but due to security concern this is also being replaced. Those who have used have used this link as a fail over link and it will operate only when the primary link fails.

Few banks are using HDLC lease line. This is being provided by Nepal Telecom. But due to support problems, it is being replaced with other media.

4.4.5 E-banking Services

Electronic banking service is provided by all the sampled banks. This has become mandatory for the banks to provide to retain customers and attract more customers. Most of the banks have provided SMS banking, Plastic card, ABBS. Internet banking has not become common, but still some banks have provided this service.

Plastic money especially debit card which is also known as ATM card has become common to most of the customer. It is the most used electronic banking service in most of the banks. Most of the banks also hold their own ATM. Generally banks hold 5-10 own ATMs. All banks have connected their ATMs in shared network. Due to sharing of ATMs, customer can make transactions from any of the ATMs in banks network. Banks charge certain amount on transactions on ATM which are not owned by them. The most shared network in Nepalese banking sector is SCT network. This network is shared by more than 75% of the banks. Other shared network is VISA network. This is shared by around 3 Nepalese banks. Customer can also make transactions from ATMs located in India. SCT shared network is also shared in Panjab National Bank of India, so people can make transactions from the ATMs in PNBs' network. VISA Cards can be operated in VISA network in India. In plastic money, banks have provided Debit Card, Credit card and prepaid card. The functioning of prepaid card is similar to credit card. Customer deposit the amount in the bank and banks provide the prepaid card equivalent to the deposited sum.

In internet banking, most of the banks have provided informational and communicative services. In informational services, customer can get the information about the banks, services provided by the banks, exchange rate, interest rate etc. Customer cannot see their account details.

In communicate website, customer can view their account information. They can view statement, balance of their account but they cannot make transactions.

Only few banks have provided transactional service in their internet banking. In this service can make transactions in their account. They can transfer fund to another account in the banks. They can pay bills of telephone and mobile via internet. But due to security issues, this service is limited by most of the banks.

Similarly ABBS is also used by most of the customer in banks. In this service customer can deposit and withdraw money from any of the banks branches located in different locations.

4.4.6 Human Resource of Information Technology

Competence of human resource of information technology in banking sector is not found well. Most of the people who are working as IT staff are from management and other faculty. Very few of these people have formal training of Information Security and Technology. Those who attended the training have also taken about the operation of the banking software. The specialized information technology trainings such as Certified Network Associate, Network security, Information Security, data base administrator etc. is not taken by these staff. It is found that most of the people are from Management background, some from IT background and few from other faculty also. Among these staffs, most have 2-5 years of experience in Information Technology related areas. Most holds bachelor degree. Due to lack of expertise, most banks have not developed Information Technology and Security policies and plan. They are doing the work on ad hoc basis. Due this, non alignment of Information Technology as per the business requirements may occur. Similarly huge investment in information Technology may not give the returns to the bank in expected time.

4.4.7 Physical and Environment Security

Physical security mechanisms protect people, data, equipment, systems, facilities, and a long list of company assets. Information security without proper physical security could be a waste of time. For physical security, generally control is placed to protect from external and internal intruders, data centre where the critical hardware of the banks are placed are secured against water, fire etc. A back up of electricity is placed which not only helps to operate the system when the power is out, it also prevents the hardware from malfunctioning due to frequent power outage. Following are the information collected from sampled banks regarding the physical and environmental security.

a. To secure from external and internal intruders, banks have implemented physical access control tools. Most of the banks have implemented door lock with automatic log features. They have implemented electric door system. People have to show or insert the electronic card provided to them to open the door. Again whoever enters the data centre by showing the card to the card scanner kept at the door, the system will automatically keeps the log of it which includes card no, time and date of entering. The security administrator can view this log any time he wants.

Some banks implemented Secure door but without automatic log facility. The door will be manually locked and restricted sign is placed over it. So only authorized persons are allowed to enter the room.

Few banks have implemented only door lock control. The door lock with security guard option is not found to be implemented by the bank. Access control mechanism implement by most of the banks are found to be sufficient to protect against internal and external intruders.

b. To protect from the flood, banks prepare the data centre above the ground floor. To protect from terrorist or accidental damage of the server and data centre, data centre is placed at the back side of building. In sampled banks, most of the banks have prepared their data centre above the ground floor and at the back side of the building. One bank has set up the system at the basement or on first floor. The data centre of the most of the banks is secured against the flood and terrorist activities.

c. Protecting the electronic equipment is essential to secure the data stored in electronic media. The electronic media and the data stored in it will be damaged when power goes out abruptly. So securing the data and equipment against power outage is important means of physical security. All of the banks have prepared UPS and Generator for power back up. As long time load shedding occurs in Nepal, UPS only cannot provide enough power supply in case of load shedding. UPS can provide electricity, for around 1 hour only for the entire system. In some banks, UPS back up is also prepared for more than 4 hours. To provide electricity at time of long time power outage, generator is placed. This can provide electricity for more than 3-4 hours also. The power back up in Nepalese banking sector is found to be satisfactory.

d.Automatic detector and logger are very important to detect and trace the events in data centre. The commonly used detectors are smoke and humid detector. Smoke detector detects any smoke generated in the room. If it detects the smoke, an alarm will ring and necessary step will be taken by the security administrator. Moisture absorber absorbs the excess humidity in the data centre and thus protects the equipment from damage. To trace what events occurred in the past, CCTV is placed in data centre. In sampled bank, most of the banks have placed CCTV in their server room. Few banks have placed smoke detector and none of the banks have placed moisture absorber in data centre. The detectors and loggers controls are not found satisfactory at an average.

4.4.8 Logical Security

a. Password Security

Weak Passwords can be compromised and must be protected. A password is generally called weak if it contains only few characters, is a dictionary word, is phone number, cell number, name of the place, name of the events etc. To make the password strong it should have contained a mixture of characters, number and special characters and it should not be a dictionary word. Moreover to make the password strong, users can be periodically forced changed, or one time password can be set. From the study it is found that most of the banks have implemented minimum length control, periodic forced changed and change on first use password policy. Very few banks have implemented password policy as alphanumeric with special characters and none of the bank has employed one time password. Most of these controls are automatically controlled by the system.

b. Virus Security

A virus is a program that requests the operating system of a computer to append it to other programs. In this way the virus propagates to other program. Virus can be easily transmitted such as a file. A virus can be deleterious which makes the system in operative, deletes program and files. Some virus can send data to unintended party via network. So virus protection is very much important in mission critical systems such as banking system. The sampled banks have applied following measures to control the virus in the system.

S.N	Control Measures	Steps
1	Preventive	a) Check new software with antivirus before its installation. b) Check new files with antivirus before they are used. c) Download software or files only from reliable source.
2	Detective	a. Regularly run antivirus software to detect the infections. b. Regularly update the antivirus program with new

		virus definition.
3	Corrective	a) Daily clean backup. b) Run antivirus program to remove infections.

Table 8 Virus Security Measure Steps

c. Virtual Private Networking

Most of the banks outsource the public shared network for branch communication. They also make branch communication using internet which is a public network. To make the transactions made through the public network environment, branch uses virtual private networking technology which encrypts the critical data transmitted from the network. From the research it is found that most of the bank used VPN in branch connectivity. Some banks also make transactions via internet; in that case also they use VPN. A few banks make the transactions via public network without using VPN. According to them, with the application of VPN, the connection becomes slow.

d. Firewall Protection

A firewall is a hardware or software that screens incoming network traffic and allows or disallows the traffic based on a set of rules. Firewalls normally sit at the perimeter of an organization's network, protecting it from the Internet, business partners, or other less secure network segments. But firewall is also kept at the point of connectivity of server and the branch network. Firewall is also used to protect from virus and other malicious programs. it is found that most of the banks have used firewall to protect from public network and even in inter branch connectivity. Some banks have also used firewall at the point of internal LAN to the server. According to them this will screen the virus that might spread from the use of Pen drive. It is found that all the banks have used firewall in the network connectivity.

4.4.9 Security in eBanking

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. The emerging eBanking application is internet banking. In Nepal also, most of the commercial banks offers internet banking. Some banks provide only the information about the banks i.e. informative internet banking. While most of the banks offer communicative internet banking whereby customers can view their account information such as balance, account statements, EMI of the loan etc., some banks also offer transactional internet banking where customer can transfer fund from their own account to their account or to the third party account. In transactional internet banking, the security of transactions becomes critical. In Nepal, the banks which have provided transactional capabilities in their internet banking have implemented following security measures.

S.N	Type	Security Measures
1	Internet Banking	• Strong Password policy • Digital Signature • Firewall Protection • Transactions within own account only.

		• transactions daily limit control • Transactions within the banks account only. • Periodic password change.
2	Authentication in internet Banking	• Multilayer password • Customer to be present to change and make the accounts for transactions. • secret questions
3	Security in Debit Card	• PIN required to enter • signature verifications • card expiry • card blacklist

Table 9 Security in e-Banking

4.5 Limitation of existing system

i. Limitations in eBanking Services

a) SMS Banking

- Information can only be viewed no transaction facilities via SMS.
- Two accounts will be difficult to integrate in single mobile number.
- The quality of the service is poor and some time no replies come when inquired from SMS.

b) internet Banking

- Limited banks have offered transaction capabilities.
- Transactions can be done within the bank only.
- Single factor authentication is done for authenticating the internet banking customers.

c) Plastic Card

- Magnetic strip cards are used in which encryption is not done and so more chances of frauds.

d) ATM

- The uptime of ATM machine is very low. Though they are said to be 24 hour uptime, they are not found as specified.
- The liquidity problem in ATM usually occurs at holiday time.
- The operation of ATM at office time is not satisfactory.
- ATMs are concentrated on city areas only.

ii. Limitations in Security Mechanism

- No Information Security plan and polices are prepared by the banks.
- Lack of dedicated information security officer in Information Technology department.
- The investment in Information Technology is not done by preparing short term and long term plans.
- Lack of Information Risk assessment and Risk management practice.

- No information security audit methodology.
- Lack of certified security personnel in banks.
- Lack of disaster recovery plan which may delay the resumption of the banking operations in case of disaster.
- Lack of expertise in particular hardware, software and other networking devices.

4.6 Major finding of the existing system

A. IT infrastructure

The IT infrastructure includes hardware, software and networking connectivity. Banks have implemented the latest hardware technology as per the requirement set of by the concerned software service providers. The main hardware is servers and security hardware. Banks have installed IBM, SUN, HP etc. servers. They are installed according to the standard set by the core banking system providers. These hard wares are providing the expected efficiency.

The security hard wares banks are using are Fort iGATE Firewall, CISCO PIX firewall and CISCO routers. Firewall is configured to protect the system from virus and other intruders. It is found that most of the banks have kept their firewall at the gateway between public network and banks internal network. Some banks have also kept the firewall between the branch connectivity and banks internal network. But the practice of keeping multi layer firewall is not found in the sampled banks. Fort iGATE firewall is implemented to control at application layer. File filtering is founded to be done by this firewall where as CISCO PIX firewall is used to control at network and transport layer.

The sampled banks have installed the latest state of the art software for their core banking activities. Globus, Pumari, Finacle are the software used in the sampled banks. Besides the core banking, they have also used back office software, share management software and HR management software. Most of the operations in banks are found to be automated.

For inter branch connectivity banks have used primary and secondary communication links. The most used communication links are Fiber Optic, HDLC Lease Line, V-SAT, Dial up, Radio link etc.

B. EBanking

EBanking is the delivery of new and traditional Banking products via electronic interactive communication channel. In Nepal following eBanking delivery channels are available.

- **Telephone Banking**

This service was started in Nepalese banks, but this has become obsolete in Nepalese Banks.

- **PC Banking**

This eBanking was never started by Nepalese Commercial banks.

- **SMS Banking**

SMS banking service is started by most of the banks. However this facility is limited to only communicative and informational. Customer can view their balance, statement and some other data such as interest rate, exchange rate etc. The transactional capability via SMS does not exist in Nepalese banks.

- **Plastic Card**

Plastic card includes debit, prepaid and credit card. Debit card facility has been offered by most of the banks in Nepal. Only few banks have offered prepaid and credit card service. The plastic card issued in local currency can be operated in Nepal and India. VISA, VISA Electron, SCT, Master Card are issued in Nepal. Most of the banks issue SCT and VISA debit card. Credit card is issued as VISA card.

- **Internet Banking**

Internet banking can be of informative, communicative and transactional. In informative internet banking, the banks website published different information about the banks such as interest rate; exchange rates etc. i.e. that information which is mainly used for marketing.

In communicative internet banking customers are provided the facilities to view their balance and account statement. They cannot make any transactions.

In transactional internet banking customer can make transactions i.e. transfer fund from one account to another.

Most of the Nepalese banks have offered communicative internet banking, some banks have started transactional internet banking also.

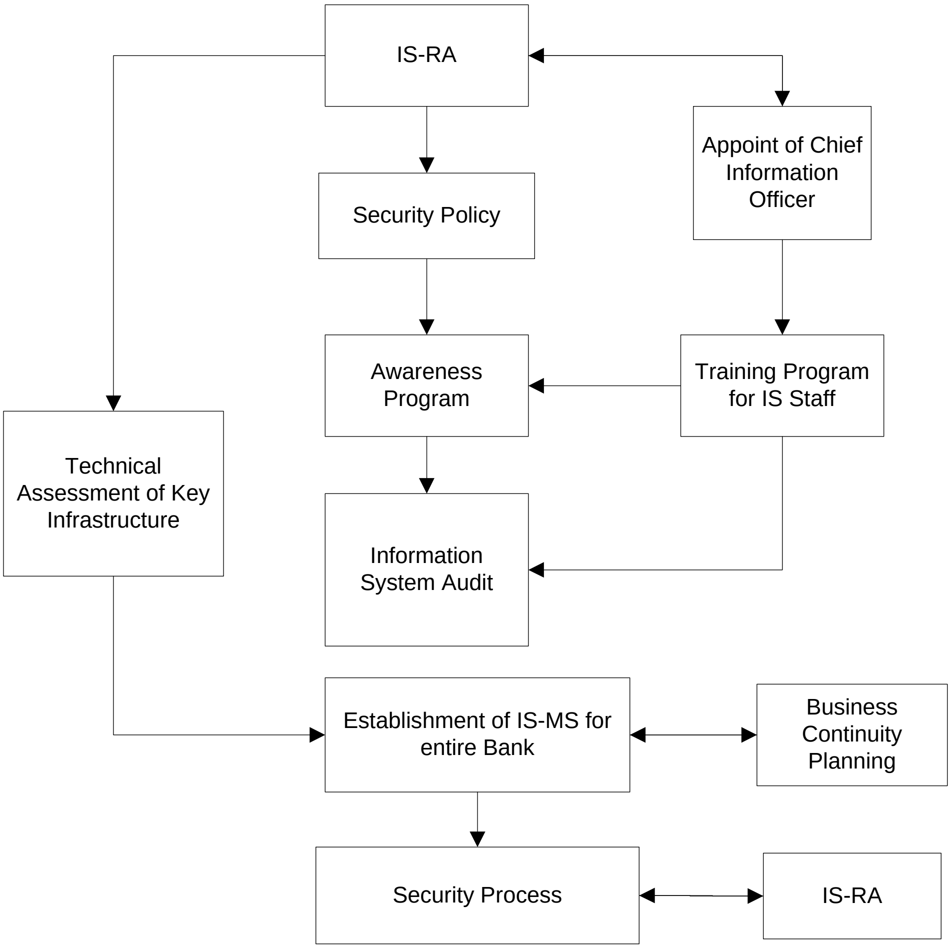
C. IT Security

Security is critical component of Information System in any organization. Managing IT security involves physical, logical security and process and procedures to do so.

- To physically secure the data and hardware equipments, banks uses secures data center. The critical hard wares are kept at secured location which is made physically inaccessible by unauthorized party by placing electronic and manual door lock system. To protect from humidity, they have not kept any electronic humid detector and absorber. To protect from power outage and power fluctuations, UPS and generators are being used in banks.
- To logically secure the system, banks have implemented password, firewall, antivirus and encryption technology. To make the password system more secure, strong password policy, and periodic change enforcement is used. Database system of the core banking applications are separated from external and internal networks by placing firewall at gateways which is used to control unauthorized access in the system from external and internal intruders and virus. To make the critical data secure while in transmission link, they have implemented encryption technology by using VPN and SSL encryption. Virus protection is provided by preparing preventive, detective and corrective virus control.
- To provide security in e-banking activities such as internet banking and plastic card, banks have implemented strong password policy

and secure PIN. Strong passwords such as minimum 6 characters length, periodic change enforcement and change on first use controls are used. To provide security for card operation, banks have implemented, secure PIN, two factor authentications etc. Some Cards can be used at POS machine without entering PIN, to secure this transaction; banks have implemented signature verification system.

4.7 Concept of new system or modified the system



IS-RA
Security Policy
Appoint of Chief Information Officer
Awareness Program
Training Program for IS Staff
Technical Assessment of Key Infrastructure
Information System Audit
Establishment of IS-MS for entire Bank
Business Continuity Planning
Security Process
IS-RA

Figure 10 Work Flow Diagram of New System

IS like any other practice has certain best practices to be followed. Best Practices would not only confine to technical configurations and settings but policy and procedures as well.

a. Information Security Risk Assessment (IS-RA)

IS-RA includes identification of critical information (both paper and electronic), their threats and their vulnerabilities. It also identifies their availability requirements vis-à-vis security requirements so as to not to compromise on availability of certain information which cannot take any downtime. It also includes identifying the maximum possible loss if certain events were to happen, thereby helping the organization taking measures to mitigate that risk.

b. Information Security Policy

An information security policy can be defined as a master document mainly containing two parts. One part contains the management's security strategy and key information assets identified during the IS-RA. The second part contains the practices, policies and procedures that the organization should follow. While the first part is strictly confidential, the second part is supposed to be circulated to all staff members.

A security policy should follow after an IS-RA so as to be effective, as a policy should have a defined objective of mitigating risks identified during the assessment. In cases where IS policy has been devised without an IS-RA, efforts should be made to align the policy towards the business objectives of the organization by conducting an interim assessment for this purpose.

One more feature to be observed in IS Policy is the top-down approach wherein the senior management decides on the practices and procedures to be followed at the Branches. Here caution needs to be exercised in getting adequate feedback from the Branches and users at various departments before introducing them in its entirety. This ensures that the policy is relevant and also stems ownership amongst users to follow the policy.

c. Appointment of Chief Information Security Officer (CSO)

Despite the growing requirements of Information Security in Banks, despite technology being embraced by Banks in such a fast pace, many Banks does not have an exclusive officer to report to the CEO of the Bank on IS.

d. IS Awareness

It is said that security is as strong as its weakest link. IS often confused with hacking and little is done with good practices. But IS can be achieved by proper and effective practices. The first step is awareness among the staff of IS and the need for the same and how they could contribute towards this objective. Further awareness should not be confined to only password management. It should entail incident response procedures (which may form part of the security policy), disaster recovery procedures and data classification.

e. Information System Audit

Information Systems Audit and Information Security Audits, though often used interchangeably are different. Information Systems Audit is independent appraisals of internal controls to assure the management, shareholders and the auditors of the company that the information provided by the system is accurate, valid and reliable. Such audits may be based on proprietary business process risk control and analysis methods. Information Security Audits is the process of evaluating practices and procedures followed by the organization and comparing them with the best practices accepted and followed and gauging the level of compliance.

f. Technical Assessment of Key Infrastructure

One of the processes in an IS-RA is identification of information that is critical to the existence of the organization. The key infrastructure where these information assets reside is identified. A vulnerability assessment could be conducted for key infrastructure to identify and rectify any vulnerability which could be exploited to compromise on the security of the information.

g. Establishment of IS-MS

After a Bank takes all the above steps, the next step would be establishing a system of continuous identification, monitoring and correction. This is because security is a discipline and not an outcome. While establishing ISMS the security best practices are enforced so as to ensure that the system is established.

h. Business Continuity Planning (BCP)

BCP is a very critical part of the Information Security Management System. It is a plan which is prepared and tested to ensure that in any uncertain event happening, the business of the organization is not disrupted.

4.8 Comparison between new and existing system

New system will have following characteristics.

- Information Technology counts significantly in the operation risk of the bank. If a system is developed to assess the risk associated with IT activities, banks and financial institutions can manage those risks easily. So the new system will have risk assessment and risk management system.
- Due to the lack of policy and procedure of Information Security, the security mechanism of the banks has not been efficient. With the policy and procedures in place, these organizations can implement advanced and efficient information security mechanism.
- There should be a responsible person to undertake responsibility and implement the policies. Due to lack of designated information security officer in banks, the practices are not followed by the staffs. With the designation of IT security officer in banks, the policies and procedures will be updated and implemented.
- All the staffs of the banks are not always informed about the latest frauds and other security awareness programs. It is thus necessary to provide security awareness program to the staffs of the bank. New system focuses on this program also.
- Regular audit of the system is also essential to confirm whether the said policies and procedures are followed by the staffs and to know the security lapses in the system .The new system gives priority for this process also.

4.9 Justification of the new system

The function of Information Technology in Banking sector has been changed from supporting factor to driving factor. New products based on Information Technology are evolving day by day in banking industry. Moreover; most of the operations in the banking sector are automated. All information are stored and transmitted electronically. The use of information Technology not only facilitates the operations of the bank, it also brings along concerns on the privacy, confidentiality and integrity of information. It is being seen that such concerns have a major impact on the functioning and existence of banks and financial institutions. While many banks in Nepal have taken steps to improve their Information Security much can be done to improve them further. It is often perceived by the management of banks that Information Security is technical and complex. The fact on the contrary is that Information Security is just like any other area of managerial decision.

The basic information security needs of banks and financial institutions are very similar to these of most large organizations. The problem in the banks is that they are fairly high value targets. A robber, when asked about his favorite haunt, said, “Banks, of course-that’s where all the money is.” Gaining unauthorized access to a bank customer records can make identity theft easy on a large scale. Unauthorized access to customer creates operational, legal and reputation risks for banks. A structured Information Security Risk Assessment will enable banks to accomplish this objective. A return on investment in Information Security should be demanded by the management. Further banks should approach information security in a structured manner. Taking initiatives without a linkage with the current environment would be unrewarding

CHAPTER - V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

This chapter summarizes the whole study in three sections. Section first includes the summary of the study. The second section presents the conclusion of the study. The third section includes some recommendations provided to the Government and regulatory body and commercial banks.

5.1 Summary

Bank and financial institutions are technology intensive organizations. The use of technology in Nepalese banking sector is increasing. The trend of automation is increasing. They are using latest hardware, software and communication medium. All i.e. Standalone, centralized, distributed and decentralized banking solution is adopted by Nepalese banks. They have mostly using extended start network topology with optic fiber, HDLC lease line, wireless and VSAT as medium of communication. The use of Information Technology not only brings advantages and provides ease in working, it brings risk as well. To minimize the risk associated with Information Technology, organization should use good and latest security measures also. Both the physical and logical security measures are adopted by the Nepalese banks. For password security, antivirus security, firewall protection etc are the measures adopted for logical security in Information Technology. But use of technology and products only is not sufficient for sound security measures. The use of policy, procedures and standard practices are equally important. From the study conducted over them it is found that the Nepalese banking sector needs to concentrate their effort in developing policies and procedures as well.

Nepalese banking sector has not followed any of the established standard of Information Technology security practices. The central bank of Nepal, which is the regulatory body of the financial institutions also, has not issued any directives regarding the information security practices, neither any guideline. The central bank has issued few circular regarding information technology but not about the information security.

Due to lack of guidelines and directives from the regulatory body, banks are getting difficulty in implementing security policies. Similarly, lack of financial transactions laws and act has also become problems for the banks to implement information security. Not only this, the lack of expertise in Nepalese market is also prominent in implementing international security policies and practices.

The study is based on mainly primary data but on secondary source of information as well. The study of existing Information Technology Infrastructure and security measures was accomplished by using primary data from the sampled banks. The data was collected from questionnaire as well as from manuals, procedures and policies.

In this way, survey of respondents has been accomplished by using primary data of 25 respondents. The respondents were selected 5 from each sampled banks. The sample was taken place by choosing banks on the basis of use of technology. Two sampled banks were using centralized banking solution, two were using decentralized banking solution where as one was using standalone system. The sample was done to represent all of our banking system as far as possible.

5.2 Conclusion

The Nepalese banking sector are using technology intensively. The way information technology is used in the banking and financial sector has been changed these days. Previously IT was supporting factor of the bank and financial institutions. But these days the role of Information Technology has been changed and its function of supporting have changed to driving function. In Nepalese financial sector also the case is similar. New products based on electronic channel are lunching day by day. SMS Banking, Credit/debit/prepaid, ATM, internet banking all is banking solution based on electronic channels. Latest hardware and software are in use in this sector. The latest distributed and centralized banking solutions are in use. In the case of hardware also, the latest servers and communication devices, firewalls are in use.

But the security measures adopted by the banks are found in sufficient. All of the sampled banks do not have security policy formed and implemented. All the security measures available in the software itself are also not implemented. The use of plan and control procedures is found to be lacking.

The human resource on Information Technology is also not found to be with satisfactory expertise. Most of people are from other background than the Technology background. The technology people are limited to only to a few and in junior position.

From the study, this researcher came to the conclusion that there are problems in the security measures implementation in Nepalese banks. The use of technology not only provides key competitive advantages; it can also jeopardize the success and sustainability of the organization if not properly managed and secured. The security in financial sector is obviously a very critical part. It is the time for the Information

Technology head of the commercial banks to focus on designing good security policy and its implementation. For security measures, the use of administrative control such as segregation of duties, job descriptions, check maker concept etc are equally important.

5.3 Recommendations

I. Recommendation for Government and Regulatory body

a) *Formulate Information Technology related Act and directives*

The transaction occurred in financial institutions should be legally acceptable. For this Law is necessary from the government in this regard. The present information technology law is not sufficient for financial transactions. Moreover financial institutions are regulatory body namely the central bank. All the eBanking services and transactions from eBanking and transactions security should be regulated by this regulatory body. The Nepal Rastra Bank which is the central bank of Nepal has not issued any directives or circular regarding transactions security and service quality from ebanking services. Due to this the ebanking services offered by the Nepalese banking sector is not found be to providing satisfactory level of availability to the customers. Moreover, the standards of operating procedures are also not at similar level in all banks. Due to lack of directives from regulatory body, banks are found not be aggressive in providing eBanking services. Thus it is highly recommended to issue financial transaction related act and directives from concerned body as soon as possible.

II. Recommendation for Commercial banks

a) More features on SMS banking

Nepalese banks have started SMS banking whereby customer can view the account information and other information such as exchange rate, interest rate etc. by sending message from their mobile phone. But transaction facility has not started in SMS banking. Mobile phone has become a common and widely used service in Nepal in these days. People even in remote area of the country have access to the mobile phone. The mobile phone is also spreading widely even in more remote areas. That is why SMS banking will be more accessible than the other electronic banking in Nepal. If transaction facility can be started in SMS banking service, people in the remote areas of the country can also pay the tuition fee of their child, can pay their telephone and mobile bills. Thus transaction facility in SMS banking will be more accessible to the people of Nepal.

Inter-bank Transaction facility in internet banking

The clearing house of Nepal is manual. Banks have to go to Nepal Rastra Bank to settle the checks of other banks deposited in their bank by their customer. If this clearing house is automated, the settlement process can be done online by using computers i.e. internet banking. Moreover, customer can do inter bank transactions by using internet. This will be a new milestone in the history of electronic banking operation in Nepalese Banks. This will save money and time of banks and customer.

Smart card instead of magnetic stripe card

All the electronic cards i.e. debit, credit and prepaid cards used in Nepal are magnetic stripe card. The storage capacity of magnetic strip card is limited due which all the information stored in this card in plain text format. This leads to easy counterfeiting of the cards. Where as the smart card stores the information in electronic chip and information in this chip can be encrypted. Thus smart card is more secure than magnetic strip card. If magnetic strip card can be replaced by smart card, the counterfeiting of debit and credit card can minimized.

b) More reliable service

The eBanking services provided by the commercial banks are not found reliable. They frequently becomes down due to different reasons such as power failure, link down and equipment failure. To attract more and more customers to use eBanking facilities provided by the bank, it should be reliable. If the present status of reliability does not change, customer might distract from the services and the investment made in eBanking facilities by the banks might go in vain. So banks are recommended to make their services more reliable.

c) Security in Mobile and Wireless Services

As banks adopt multi-delivery channels in response to customer demands for greater convenience and lower costs, the wireless channel has seen growing acceptance in the retail payments, although it still varies across geographies. This is being driven by the ubiquitous nature of wireless devices and their consumer acceptance, and the benefits of convenience and low transaction costs. Also, with the intensification of competition, the industry is increasingly feeling the need to equip its mobile workforce with mobile or wireless devices to boost efficiencies and improve customer relationship management (CRM).

Wireless local area networks (WLANs) are increasingly becoming popular because of the flexibility and mobility they provide. With the increased benefits and convenience of mobile and wireless applications in the banking industry come increasing risks in security and the need for security solutions. Three points of security vulnerability exist: the mobile device itself, the wireless channel, and the network connection between the wireless web servers and the back-end transaction servers. Handheld devices and wireless local area networks (WLAN) are especially vulnerable to potential viruses and the ability for wireless signals to be picked up beyond their intended recipients. Thus, stricter security policies, WLAN security upgrades, the use of encryption technology such as virtual private networks, and end-to-end security solutions are highly recommended.

d) Implement International standards of information Security

There are international standard for information security. The standard includes different security measures that should be implemented by the technology intensive organizations. The most used international standards are COBIT and ISO standards. Banks can use any of the international standards that are suitable for banks. It is recommend that bank should study on international information security standard and follow any one of them.

BIBLIOGRAPHY

Acharya I. (2002). *Implementation of MIS at RNAC- A case study in marketing department*, An unpublished master's degree thesis, Shankerdev Campus, T.U.

Adhikari Shankar (2005). *Introduction to Management Information System*, Kathmandu: Buddha Academy Publishers and Distribution Pvt. Ltd.

Anu Sunil (2005).*Information System of C-MODE Inc.* , An unpublished master's degree thesis, Shankerdev Campus, T.U.

Bhattarai A.P (2003). *Performance of MIS in Kumari Bank,* An unpublished master's degree thesis, Shankerdev Campus, T.U.

Bollapragada, Vijay, Mohamed Khalid, Wainer Scott (2002). *IPSec VPN Design*, USA: Cisco Press

British Standards Institution (1995). *Information Security Management, Part 1: Code of Practice for Information Security Management of Systems (BS7799: Part 1: 1995).* London: British Standards Institution

Federal Reserve Bank (1999). *Internet Banking, Comptroller's Handbook*, Washington: USA

Finacle System (2002). *Managing Security in Mobile and Wireless Services*, India

Gordon, J. & Gordon, S. (2000). Structuring the Interaction between IT and Business Units: Prototypes for Service Delivery, *Information Systems Management*, Vol. 17: No. 1, Hada, Sunila (2004). *Credit Card Practices in Nepal*. An Unpublished Master Degree Thesis, T.U

Hodgkinson, S. (1996). "The role of the Corporate IT Function in the Federal IT Organization", *Information Management: the Organizational Dimension*, New York: West Publishing Company.

Jawasker W.S.(2002). *Management Information System: 2nd Edition*. New Delhi: McGraw Hill Publishing Company Limited.

Joshi, Neeru Baba (2000), *Management Information System in Nepalese Banks: Case Study of RBB,* An unpublished Masters Degree Thesis, Shankerdev Campus, T.U.

Julia H Allen (2001). *The CERT GUIDE to System and Network Security Practice.* New York: Addison Wesley, pp.512-520.

Khadka Ashis (2004). *MIS and its application in HMG/DANIDA*, An unpublished master's degree thesis, Shankerdev Campus, T.U.

Klevinsky T.J., Scott Laliberte, Gupta Ajay (2002). *Hack I.T.: Security Through Penetration Testing*, USA: Addison Wesley

Lamsal A. (2003), *Information System Design: A case study of Agriculture Development Bank Nepal,* Kathmandu: An unpublished master's degree thesis, ShankerDev Campus, T.U.

Manandhar N. (2007). *Design Process of Mobile Banking Service (Management Information System),* Kathmandu: An unpublished Masters Degree Thesis, Shankerdev Campus, T.U.

Omar Santos (2008). *End-to-End Network Security Defense-in-Depth*, USA: Cisco Press

Raghuvanshi Keshab (2006). *MIS in cable Television Organization,* An unpublished master's degree thesis, Shankerdev Campus, T.U.

Robson, W.(1997). *Strategic Management and Information Systems: an integrated approach*, USA: Addison Wesley

Ron Weber (2006). *Information Systems Control and Audit*. New Delhi: Dorling Kindersley.

Shrestha, Madhu Sundar. (2007). *Fundamentals of Banking*. Kathmandu: Buddha Academic Publishers and Distributors Pvt. Ltd.

Shrestha Raja Ram (2006). *MIS in Benchmark Pvt.Ltd. (A Case study of Computer Maintenance Information System)*, An unpublished master's degree thesis, Shankerdev Campus, T.U.

The Commonwealth Bank of Australia (2007). *E-Banking General Information and Terms and Condition*, Sydney: A brochure

Wolff, Haward K. and Pant, P.R. (1999). *Social Science Research and Thesis Writing.* Kathmandu: Buddha Academic Enterprises Pvt. Ltd.

Yibin M.U. (2003). *E-Banking: Status, Trends, Challenges and Policy Issues*, USA: Addison Wesley

Websites:

http://www.thales-esecurity.com

http://compnetworking.about.com/

http://www.techrepublic.com

http://www. wikipedia.com

http://www.adbl.gov.np/

http://www.bok.com.np

http://www.himalayanbank.com/

http://www.kumaribank.com

http://www.machbank.com/

http://www.nabilbank.com/

http://www.nccbank.com.np/

http://www.standardchartered.com/np/

ANNEXES

Annex - I

QUESTIONNAIRE

Dear Respondent,

I have been conducting a research on "*Present Status of Information Technology and Security Measures in Nepalese Banking Sector*" as a requirement for the partial fulfillment of the degree of MBS. I hope this questionnaire be an effective methodology to find out the issues of Information Technology and Security Mechanisms in Nepalese Banking Sector.

I have sent some questions regarding IT hoping that your timely response will come. So, I heartily request you to fill this questionnaire at the best of your Knowledge. Your kind cooperation in this regard will be of great value for me.

Yours faithfully,

Ajit Regmi

Tribhuvan University

Shanker Dev Campus

MBS Final Year

<u>Respondents:</u>

Name of Respondent: [optional]

Address: [optional]

Name of the employer:

Current Post:

Please check the box with '×' sign before the option where applicable.

1. **Banking System**

    a. Which banking system does your bank have?

□	1. Centralized System	□	2. Decentralized System
□	iii. Distributed System	□	iv. Mixed (specify).............................

    b. Are you satisfied with the banking system architecture?

□	1. Yes	□	2. No

        i. If you are not satisfied, which system do you think your bank should adopt?

□	1. Centralized	□	ii. Decentralized System
□	iii. Distributed System	□	iv. Others (specify)..............................

    c. What are the problems with your system architecture? (Please List it out.)

        i. ....

        ii. ....

        iii. ....

        iv. ....

2. **Software Used**

    a. What is the name of the operating system used for your CBS? (Please provide the name)

        i. ....

        ii. ....

iii. ....

b. Which database is used by your CBS? (Write down the name of software)

i. ....

ii. ....

c. Which system(s) is used for your CBS?

i. ....

ii. ....

d. How much of the functions are automated in your Bank?

	i. <50%		ii. >50%<75%
	iii. >75%<100%		iv. 100%

e. Please list the nature of security software used by your bank if any.

	i. Antivirus Software		ii. Anti ad ware and anti spy ware
	iii. Firewall		iv. Others (specify).............................

3. Hardware Used

a. What are the servers are used in your bank?

	i. RISC		ii. CISC
	iii. General PC		iv. Others (specify).............................

b. How many Servers are in use?

	i. 1-2		ii. 2-4
	iii. more than 4		

c. What security hardware is used in your bank?

	i. Firewall		ii. Router
	iii. HSM		iv. Others (specify).............................

4. Network Technology

a. Which Network Topology is used in your Organizational Network?

	i. Star and extended star topology		ii. Bus topology

	iii. Mesh Topology		iv. Others (specify).............................

b. What are the Communication Media used in your organization?

	i. Optic Fiber		ii. V-SAT
	iii. Radio Link		iv. HDSL lease line
	v. Others (P.S.)............................		

5. **E-banking Services offered.**

a. What electronic Banking products are offered by your bank?

	i. SMS Banking		ii. internet Banking
	iii. Plastic Card		iv. ABBS
	v. Others (Specify)		

b. If you have provided internet banking, what services are offered by your bank?

	i. N/A		ii. Account Inquiry
	iii. fund transfer intra customer account within bank		iv. fund transfer inter customer within bank
	v. General Information		others.....................................

c. How many ATM machine do your bank holds?

	i. 0		ii. 1-5
	iii. 5-10		iv >10

d. Does the ATMs in your bank is connected with other shared network?

	No		ii. Yes with VISA
	iii. Yes with SCT		iv. Others (specify).............................

e. What is the most use e-banking service in your banking?

	i. Debit Card		ii. Credit Card
	iii. internet Banking		iv. SMS Banking

	v. ABBS		vi. N/A..............

f. Which of the following plastic money facility is provided by your bank?

	i. Debit Card		ii. Credit Card
	iii. Prepaid Card		iv.N/A.............................

6. Human Resource of Information Technology

a. How long you are working in Information Technology?

	i. 0-2 years		ii. 2-5 years
	iii. 5-10 years		iv. >10 years

b. How long you are working in your current post?

	i. 0-2 years		ii. 2-5 years
	iii. 5-10 years		iv. >10 years

c. What is your faculty of education?

	i. Management		ii. Information Technology
	iii. IT related field		iv. Others (specify).............................

d. What is your qualification?

	i. Masters		ii Bachelor
	iii. Intermediate or less		iv. above masters

e. Have you taken any special training to handle your job more qualitatively?

	i. Yes (P. List below)		ii. No

7. Physical and Environment Security

a. How is your server room protected from external and internal intruders?

	i. Door Lock with restricted sign		ii. Door Lock only
	iii. Door Lock with security Guard		iv. Door Lock with Auto Log facility

b. Where is your Data Centre Located?

	i. First Floor on back side		ii. First Floor on Front side of Road
	iii. Ground or basement on roadside		iv. Ground or basement at backside

c. How is your Equipment protected from high voltage and power outage?

	i. UPS with Generator Backup		ii. UPS only
	iii. CVT		Others(Specify)

d. Is your server room equipped with electronic detectors and loggers?

	i. CCTV		ii. Smoke Detector
	iii. Moisture Absorber		iv. N/A

8. Logical Security

a. What password policy is practiced to access the system?

	i. minimum length control		ii. combination of alphanumeric
	iii. alphanumeric with special character		iv. periodic forced change
	v. change on first use		vi. Others

b. How virus is controlled in the system?

	i. Preventive Measures		ii. Detective Measures
	iii. Corrective Measures		iv. Others (Please specify)

c. Please check if where VPN is applied?

	i. branch connectivity		ii. connection to server via internet
	iii. No VPN		iv. we have private network and VPN necessary

d. How is firewall configured to protect the system?

	Public network access is firewall protected.		ii. Inter connectivity is firewall protected

	iii. Access to the server is firewall protected even from internal LAN		iv. Others (specify).............................

9. Security in E-banking

a. What is the security mechanism applied for internet banking?

	i. Strong password policy		ii. Digital Signature
	iii. firewall protection		iv. Others (specify).............................

b. How the transaction in internet banking is secured?

	i. Multi layer password		ii. Customer to be present for account update
	iii. two factor authentication		iv. Others (specify).............................

c. What is the security mechanism applied in debit card use in POS machine?

	i. PIN required to enter		ii. Signature Verified
	iii. Photo Verification		iv. Others (specify).............................

Sampled Commercial banks

i. Kumari Bank Limited

ii. Nepal Industrial and Commercial Bank

iii. Agriculture Development Bank Limited.

iv. Nabil Bank Limited.

v. Everest Bank Limited.

Annex- II

1. C Problems with system architecture

S.N	System Architecture	Problems
1	Centralized system	• Single point failure • Problems in network medium causes halt of operation at branches. • Problems in creating UserId soon. • More than two back up of the network medium needed.
2	Decentralized System	• No manpower of IT at each branch. • Separate System room with special security needed in branches. • Same operation repeats at each branch. • Difficult to provide ATM facility and ABB facility to any branch. • Difficult to set up Disaster Recovery Site for each branch. • For each branch separate hardware and software needed and taking license software for each branch is costly. • Difficult to setup security solution such as antivirus for each branch.

2. Software Used

S.N	Application	Software
a	Operating System	Sun Solaris, Ms. Windows
b	Database	Jbase, Ms SQL, Oracle, Ms. Access
c	Core Banking System	Finacle, Globus, Pumari Plus

Annex- III

Responses to the field survey based on Questionnaire

Q.N		Option wise Response						Total Response	Remarks
		i.	ii.	iii.	iv.	v.	vi		
1	a	9	6	0				15	9 Respondent Answered Yes
	b	4		2				6	
	c	Annex II							
2	a								
	b								
	c								
	d	0	5	10				15	
	e	15	12	6				33	Respondent answered more than one Option
3	a	12	0	3	9			24	
	b	0	3	12				15	
	c	15	15	12				42	
4	a	12			3			15	
	b	15	9	9	6			39	
5	a	12	12	12	15			51	
	b	3	12	6	6	12		39	
	c	6	3	3	3			15	
	d	3	9	6	0			18	
	e	12	0	0	0	0	3	15	
	f	12	3	3	3			21	
6	a	4	6	3	2			15	
	b	8	5	2	0			15	
	c	7	5	2	1			15	
	d	4	8	3	0			15	
	e	12	3	0	0			15	
7	a	3	6	0	6			15	
	b	12	0	0	3			15	
	c	15	0	0	0			15	
	d	6	3	0	6			15	
8	a	12	9	3	6	9	3	42	
	b	15	15	15	0			45	
	c	12	3	3	0			18	
	d	12	12	6	0			30	
9	a	12	12	12	0			36	
	b	12	12	0	0			24	
	c	9	3	0	0			12	