CHAPTER 5

ISSUE OF MIS SECURITY

5.1 DEFINE MIS SECURITY AND DIFFERENT ORGANIZATION

5.1.1 DEFINE MIS SECURITY AND ETHICLA ISSUE WITH SUGGESSION

MIS security is word of protecting information system with specific rules and strategy based policy applied in data warehouse. With managing all functional department data security is the important concern of entire database. Complete responsibility of data protection on network of interdepartmental and from public network. Amount of process involved within organization and with vendor and client who are business contacts for communication all such interference need to monitor and its logs has to be recorded for further reference. Security maintained on each level of communication support the privacy policy of organization. Information system and data mart contain different source of server of functional database through which people are connected for many business process transaction. Users also communicate on public network for mailing purpose or even for web search for surfing business related database. To protect private organization’s intranet from the outside world with secure software and firewall policy on server. Information system security is the protecting technique against unauthorized access on computerized network.

Information system security has aspect in technology protection concern and data protection concern over the network. **Technology protection concern** can resolved with the support of security against malicious cyber attacks and try to protect by defending. And protect the internal information system of the organization. **Data protection concern** ensures the integrity of information system of organization from physical theft, malfunctioning and backup issue. To develop effective information system security few elements are support to protect data and technology over the network. List of suggestion for information security system:

- Keep database safe from unauthorized access, without permission no one can get the access in the server room and not even on virtual sever of information system of organization.

- User has to follow the security policy for data access and even access to their system.
• They should not share the login id and password of the system to others.
• User has to follow the entire communication channel for database access.
• Monitor the logs of web access by info sec. department
• System health checkup and scanning has to be done periodically.
• Encrypt the documents when its transmitting over the net
• Ensure the digital signature for integrity validation
• Authentication and authorization access has to be update periodically
• Management has to ensure that new employee should aware about info sec policy of organization and that has to be adhering as per rules.
• Licensing software get it checked as per database
• AMC of systems timely update and monitor for better performance
• Downtime of info sec and technical team maintain monthly
• Transaction of information communication over voice or through mail it must approved to authorize manager or user of it ownership.
• Ensure data flow on network has approved and provided access to right user.
• I.T. executive and info sec executive need to work together to make secure technological communication interface in organization and even for stakeholders who are external approved access holder on web for concern information of business.

Information system security is the matter of ethics and legality in its rule. It has certain obligation over network and makes it more secure from cyber crimes and attacks from malicious access which can damaged system, server or database physically or even virtually with its threads. Hence organization information system needs to be maintained by Chief Information Officer as well as by each user of it by ad herring all the security rules of information system.

5.1.2 LIST OF ORGANIZATION IN SUPPORT TO ETHICAL ISSUE
• IEEE: Institute of Electrical and Electronic Engineering
• ACM: Association of Computing Machinery
• CPSR: Computer Professional for Social Responsibility
• AITP: Association of Information Technology Professional

Above all listed organization is professional platform of information technology and communication technology. All these association has unique role with their existence
such as IEEE code has standardized value which is ethical for professional environment IEEE provides policy with social responsibilities, it also understand the need of technological uniformity and standardize flow process all over the globe. It supports to solve the disputes between parties who involved in technological consequences due to its technical or procedural situation in engineering or in automation field of computerization. IEEE adds the competitive advantage over the network. Assign the training to the professional to become more expertise and acknowledge the technical process all over the business organization. It also protect the ethical rights from injure of reputation, property, employment by false action over the network. It adopts and amends the right changes in the policy with honest criticism in expertise filed of technology. All the employee of IEEE commits themselves with highest ethics in their professional practice and they demand it to spread all over in the society to improve the standard of living and optimum right use of technology for individual whomsoever involved in it.

5.2 ISSUES IN MIS SECURITY CONTROL AND ITS SOCIAL DIMENSIONS

5.2.1 Issue of MIS security control:
MIS is wide concept of itself. Its functional database with specific process followed for operational as well as for executive decision. Management information system security is the main concern to keep stability in organization to more productive and profitable in the process of business transition by protecting database and system from cyber attack and cyber crime and even internal unauthorized access or actions. Information system needs to maintain confidentiality, Integrity and availability within the management structure. And systems need to protect from threads, risk over the IT environment. Following is the list of issue in management information system:

- External Coercion
- Internet access
- Without firewall protection
- Public network access without permission
- Accessing unprofessional sites blogs from server system
- Internal Coercion
- Unfair practice of information system
- Password and login un-authorization
• Disclose login id and access id with password within group
• Authorities access conflict
• System not scanned in periodic method
• Un-updated antivirus
• Licensing updating not done on time
• Information security system checkup delayed
• Server maintains delays
• Server monitoring ignored
• Lack of cleaning and cooling in I.T. area where system used
• Lack of awareness in the employee and user of system and net
• Lack of training to user to use particular application software over the net
• Ignore the info sec policy and used external disk, pen drive

Hence information system security is not only the concern of I.T Officer and executive it is the matter of all individual to follow and understand about information security policy while using system, intranet, application and internet and web mail. Issue can be anything but if employees are aware about to avoid above things and I.T. and Information security department work monitor control the data and technology farm then information system will surely achieve success to keep secure environment in the organization over network.

5.2.2 MIS ETHICAL AND SOCIAL SECURITY DIAMENSION

MIS has expanded large due to its importance of information system in organization. Hence Management information system enlarges the scale of security over the network in ethical and social environment. MIS has different functional department which maintained the code of conduct because of its ethical and social element involved in the entire process. Securities dimensions of ethical and social importance in MIS are content certain obligations and responsibilities to specific entity that has to follow the security policy to monitor and control for effective performance of technology and communication use of information system.

• Responsibility of employer
• Responsibility of management
• Responsibility of Proprietors
• Responsibility of society
- Responsibility of country

Above all are the entities who are obliged to follow the rules set by specific organization in area of their technological and commercial utilization process. Its start with and end with involvement of each individual directly or indirectly to play the role of technological existence and informational use. Following point clear the above noted entity with further explanation, how security concern important in everyone’s life and its circulated and connected with system of professional act affect to lives of many in the process of business transaction and these dimension are the concerns with entire process of information system security to protect ethically and socially:

**Responsibility of employee:** every employee is entity in itself if look through the concern with the professional outlook, because employee are bounded with specific rules and policy which they have to follow as a part of organization. Hence employee are trained and informed by information security department about technology and application software they need to use in organization. Information security team provides basic training for what they are obliged to follow the rules and what policy they need to maintained over the network. Management approves the access on database to new employee on which folder or file they have to work for business transaction. All such approval process and database management are different from company to company policies depending on which type of software they are performing with business task.

**Responsibility of management:** Management is the key role of business organization which manage the entire flow of process from production to sale or data collection to feedback process. Management is the act of planning, organizing, implementing, monitoring, and evaluating to get things done. So they are the core supply the right kind of information and instruction to all employee of organization about information security and its importance in their day to day act. Management acts as the leader who performs excellence in his area of functional department hence manager instruction of information system security will be followed by the entire group. Management must organize the session and training program by information security team.

**Responsibility of proprietor:** every owner of organization has contribution to society as corporate social responsibility for organization and even for all in society. Proprietors are role model of many hence they must follow and also instruct the same information security information to entire organization. On all level of structure in
business process they update the technology and same has to be informed to employee. They need to provide funds which are needed to update the license of systems and any other application. Ethics and ethical rule are reflection from process manage in the business so proprietor have to monitor periodically on management and even all inter management employee and subordinates. They must provide and appreciation annual or monthly award and reward to the best performer employee of organization based on the criteria of following all ethical practices on network with maximum profit giving to organization by using information system and business network for business transaction. It not only improves the performance of other employee but it will ultimately intend to generate profit to organization.

Responsibility of society: to form ethical place to survive and grow with all. Such win approach of all individual will really form the effective place to grow financially as well as socially with right way to live. Society consist of the people or an individual who can be direct or indirect element as customer, vendor, advisor, reporter, auditor, employee, proprietor connect with business process so everyone has to trust on trusted sources of information system and spread what is right for all. Certain specific rules must be following on cyber network.

Responsibility of country: whenever there is matter of two country boarder both have to follow ethical rule to maintain good relationship with each other for business growth. Both countries may have different rules and policy for their employee or for organization but fundamental point will be always same on the approach of ethical and social responsibility to maintained profitable and developed relationship between different countries. Certain obligation will be there on specific task not to be allowed within boundary of country on cyber world such rule has to be followed depending on the country’s organization policy for information system security concern.

These are the dimension of business organizations which basically directly or indirectly involve in information system security to perform their role and that has to be ethical and socially accepted by corporate as well as it must approved by concern government bodies of the country. Ethics will be universally same only thing it applicable due to miss use of system, cyber network or database or information system but it’s ultimately perform through human being only. So in matter of security information system is the automated database managed by people and for people that always kept in mind to keep respect of responsibility toward society. The moral dimensions of information system are needed to protect from cyber attack. It is the
responsibility, accountability and liability of every professional and individual’s to protect the ethical practices in the daily life and it responsibility of everyone to perform the duties and accept the decision with full obligation ethically. Be accountable to follow the code of conduct by organization and legal bodies in society. And its liability of all to be aware and alert while dealing on internet not to access unauthorized sites or blogs which can damage system or program. There are many areas where moral dimension identify the human rights and duties at the level of ethical, social, personal and political phase of communication and all have to grow up with the integrity and wisdom to make this world more safe and secure over cyber world. Below are the listed areas where moral need to be followed:

- Information rights:
  - Privacy on internet
  - Freedom on internet

- Intellectual Property rights
  - Trade secrets
  - Copyright
  - patents

- accountability with liability control
  - accountability to follow organization policy
  - liability to be alert

- System quality
  - Data quality
  - System error

- Quality of life
  - Equity
  - Access
  - Boundaries

These are the area where every professional and even individual has to be clear and focus about these rights which also come up with certain responsibility and liability to know about it while browsing on internet and working online. Cyber world is place where host PC are connected on internet and accessing web server for various kind of information or for communication between client and users. Firewall security protect intranet from cyber attack there are various kind of terms of it as follows:
• Hacking
• Spoofing
• Sniffing
• Identity Theft
• Denial of service attack
• Click fraud
• Cyber terrorism and cyber warfare

To keep cyber space secure need to be following the rules and policy over the network and protect the computers and application through strong security policy. Following are the tools and techniques for security:

• Firewall
• Antivirus software
• Intrusion detection
• Access control system
• System authentication
• Biometric authentication
• Encryption and public key infrastructure PKI
• Securing wireless network
• Digital certificate
• Digital signature
• Electronic evidence log record
• Computer forensics
• Electronic record management

These above security elements work as doorkeeper but its ultimate responsibility of user that never share authentication details i.e. login id and password details or anything which helps attacker to access your system over network. Periodical scanning for antivirus keep system update and secure from malicious attack. System administrator must maintain the internal policy rules on the program to keep secure connection of internet and intranet to the each host of organization.

5.3  I.T. GOVERNANCE FRAMEWORKS

I.T. is the support center and interference between organization and communication within entire world. Modern technology has provided the platform where all
functional databases of organization are integrated due to which communication flow on application has desired connectivity and access process as management instruction to I.T. and Information system security team. Effective organization monitoring and management provide high quality output and create valuable strategic management and I.T and Info. Sec. Department collaboratively plays an important role in this. It’s possible because of particular design and framework decided for entire communication and database access system. And now days there are many organized framework through which implementation provides perfect and hundred percent output with effective process of communication between each employee who relates to management and database for accessing information system. Below is form of I.T Governance framework which shows their use will give effective and efficient output: I.T. Governance is the framework set of rules and structure which support to maintain working flow of organization with the effectively use of Information technology. It enable many success to organization based on it structural use of database and technology assign to individual over the organization network. it support to infrastructural platform which handled the technological process and it cover the policy and rule to monitor or control on acts of employee or stakeholder of organization over the network. Objective of I.T. Governance is only one goal to support IT infrastructure and help to grip the success of business strategies and organization goal and its’ vision. Its structures form various standardize design emerged with advance process and set of corporate policy to cover and support them from business uncertainty due to technological concern in business process transition. There are defined task of each organization department to get things done through adequate and complete use of information technology. I.T. has involved many functional types of user to its usage employee, vendor, customer and client with organization’s information system with assigned and approved rights of its usage. There is different area of IT Governance:

- Task governance
- Knowledge management
- IT Support management
- Technical management
- Information system management
- Service level management
• Risk management  
• Information security management  
• Regulatory compliance management  
• Business consistency management  
• Disaster recovery management  
• Project governance management  
• Consultancy service management  
• Intellectual governance management  
• Functional policy governance  
• Inventory governance management  
• Training service management  
• Choice of IT Governance standard management  
• Additional special system management  
• Incident governance management

IT Governance is the key role player in organization. All employees, managers, directors, auditors and practitioner are responsible and obligated to the usage of information system over organization network. All events and logs are monitor and control by information security team. IT Governance Library provides enterprise I.T. business strategy and its usage for specific reasons explained in details. Following are included in I.T. Governance standard framework for organization to implement:

• **ISO 27002**: ISO27002 is the information security standard used as best practice in the organization. IT Governance extended to integrated information technology with management strategy which explores the culture, value, objectives and ethics of organization in competitive environment. To achieve competitive advantage IT Governance framework can extensively collaborate two or many other framework of IT Governance. Combined the few techniques of framework of ITGS and COBIT Plus ITIL will create significant rules and policy to implement over the integrated function database and management where these collective force of framework implementation will prove best practice to regulate and corporate governance compliance.

• **ISO/IEC 38500**: It is international I.T. Governance standard which is globally accepted as formal framework pattern for corporate. This framework is specific format for information and communication technology of
organization. ISO/IEC38500 available in June 2008 and it’s developed in the lead the trail blazing work done by Australian standard institute which was printed in 2005. As organization are spread business all over the world and globally connected so to make the secure transaction for business purpose this framework accepted on international standard irrespective of geographical region. It provides policy and rules to be followed by all involved entity in the process of database access and transmission of information over the network.

- **Calder Moir**: There are many business entity which forms to solve the legal and complex matters as their service to the client and many organization started their enterprise startup at critical risk of production of product which competitors has monopoly in the market so it’s kind of risk even of loss of existence in market for organization. But information system and research plays an important role to cover risk and find competitive advantage as source of new innovation to employee to introduce with specific new strategic management step with proper I.T Governance control over the information security and control on management task these will solve the critical and complex issue of organization and Calder Moir is the framework which regulate and provide structured support on complex matter. The best quality of this framework that on each level of business process it sets the benchmark for enterprises, practitioner and researcher. It use ensure the effective output to organization with management growth in their performance and output of more innovative and practical about each step of framework. It provide IT Governance toolkit.

- **ITIL**: It is defined as Information Technology Infrastructure Library. It is mostly accepted and implemented framework strategy of IT Governance its regulatory and governance compliance support many information Security dataset structure and communication flow over the network. It was introduce by UK cabinet office where different kind of IT service management library for the best practices to implement in enterprise structure of technology and information security system. It is accepted internationally and it supported through ISO/IEC20000:2011. There are certifications to be needs to assure the expertise in its process of understanding and implementation in to the I.T. Governance business of organization. ITIL is the best regulatory framework of
incident and response management and it control many internal practices of
information technology as well as cyber world regulation possible to manage
through specific application software as service request portal of organization
to all employees and other stakeholder of the organization.

- **COBIT**: Defined as Control Objectives for Information and Technology
  which control the tools of access on database within enterprise network and to
  outsider for provided web link or specific portal of organization. This
governance mainly focuses on the controlling and measuring the process of
objective to complete with control system. It helps to enterprise to achieve
organization challenges in the field of regulatory compliance and risk of
management structure flow in technological order or assessment. COBIT is
internationally well known I.T. Governance framework which assesses and
measure the enterprise information technology potential and COBIT has
update version from 4.1 to version 5 in 2012. It also capable for the 37 defined
COBIT process of business enterprises.

- **Green IT**: In corporate organization IT Governance consider the role of
  Green IT. Green IT has important element in framework development,
decision making, and business structure and communication authority on
management level which added support policy, cutting edge texts with the
support of environmental management standard ISO14000. It Framework
support to the complex task to solve and critical risk to be solve as business
opportunity with proper regulatory policy and control the technological
process within organization.

5.4 INFORMATION SECURITY IN SDLC AND RECENT TREND OF OPEN
SOURCE DATA MINING TOOL.

5.4.1 INFORMATION SECURITY IN SDLC

Software Development Life Cycle is the managing different phase of changes in
developing program of instruction going through planning, development, and
analysis design, implementation and support phase of life cycle. Different security
adds in different level and help to integrate information security on each phase of
SDLC. NIST National Institute of Standard and Technology introduce the security in
SDLC will produce more effective result and save cost of processing in operational system. Following are the phase which defined information security in SDLC:

**Planning:** It’s primary step of software development life cycle. Security is the important concern in it and software has to understand the need and requirement of organization process and connectivity flow of communication with stakeholders so getting this information will help to decide about kind of software developer has to develop and it will available to whom on network of organization. Understand and consider requirement, security threads, and potential constraint and integration of functional database. Planning in all above area has to be considering in this level of software development, how much strong inclination between security and functional database, its level of integrity, confidentiality and availability to the user over the network. Developer has to decide and consider below mentioned point while they are in a planning phase of software development life cycle:

- Time need to develop
- Cost of primary phase of development
- Element which need to update for integration
- Requirement of business process organization
- Format of level one phase
- Consider privacy concern
- Expected process flow in the software for effective output
- Which programming language to use

**Development:** This is second level of software development life cycle where actual development process is started with programmer to generate the coding and different models in its process. Now days there are many automated basic programming integrated with the source of open source database for the use in development process. Modern tools available for development process i.e. JAD, Extreme programming and Prototyping. Even in development process developer has to complete the entire process of this phase which included following tasks:

- System purpose
- System analysis
- Computer programming
- Testing
- Production
• Maintenance

**Analysis:** This is the phase of essential action in its level of intelligence of developers. Evaluation of right choice of analysis will support to the right kind of software development for organization. It mainly analyzes to cover the risk of assessment and scope of regulatory control in software program for future precautions. It not only analyzes the organization need but also security requirements. Following are the element developer has to consider on the level of its security point:

- Functional requirement of management
- Database integration criteria
- Assessment of access concern
- Credential and accreditation over the software to user
- Conduct the risk assessment
- Control baseline need of security code
- Perform testing function
- Scrutiny over sequential components
- Check all compatibility with information technology
- Advance and adoptable combination of support tools

**Design phase:** This phase mainly draw the entire design of communication through software within organization and how that software connected to functional database over the network from the front end and back end communication to complete the business process transaction. Here security architecture involved in software designs of requirement of business processing transaction through centralized process of communication. Following point need to be considered in design phase:

- Check it synchronized with relative database
- Scope of software use
- Check the connectivity flow of communication
- Security level with management steps
- Form effective design for integrate software
- Design must not critical and complicated in overview

**Implementation:** In implementation phase of software development life cycle where software ready to test in real time scenario. Implementation is the process of stepwise modification in software in case it requires changing some tools and policy in it. This stage give the real idea about software performance whether its fail or successes in the
level of implementation. Once it successful in its implementation makes it available to user after deployment on site. Add support system in technical support department to handle user query. Following point need to keep noted in stage of implementation:

- How much downtime need for this process
- Update to user about change in or new deployment of software
- Consider the time and cost involve in it
- Check all security concern and mapping with other database

**Support phase:** After the implementation phase feedback has to be derived from concern group of members of software tester and user to evaluate the process and functioning of software development life cycle. There must be periodic maintenance and evaluation of operational system of software design and its use. It enhanced and modify the process of software system wherever require. User may need support system to understand the functions of new software system. And support team has to provide timely solution for the query this will control to fill the gap of awareness of software functions. After implementation phase user start accessing system from various sources with assigned permission over network.

Above all are the phases of software development life cycle which continue involved in the innovation process of research and software updating for further use. Above all phase can be repeatedly follow with new function tool in software to add and control the entire support system of SDLC with security database management over organization network as well as on web portal.

### 5.4.2 SYSTEM DEVELOPMENT METHODS

Software development process has many overviews about use of particular software and the process of using the system software for business process transaction. Due to advance automation in information world the use of computer emerged with the high level of technology system in information database security. Previously system developed on the structural base but now in modern time it’s more specific about object oriented analysis. Both designed effectively proceed for organization performance but object oriented analysis has advance function to control information system as it’s also based on structural oriented concept. Whereas structured analysis moreover based on the levels of communication and least bother about object to complete with the process. All steps are depends upon the approach of information
system connectivity with security framework and management assessment policy. Systems are developed to provide alternate solution form the business and find the weakness and strength of organization to control the risk and take the steps to provide compliance to the system. There is no strategy exist in the process of which are utilized universally in same pathway as run in one organization. Every organization has own functional database, process of information security system and level of management. IT Governance even accepted the fact that it’s all part of new innovation system and research and development matters in its life cycle of service. Following are the few listed software system:

- **Objective oriented analysis**: this is widely used programming methods in real scenario. Object of this software set is human resource, things, process and incident, it’s developed through programming language then it transforms the object in reusable code. System developed to retrieve the object of the whole process and all element of it connected with functional integration and management level of assigned access of authorization plays an important role of security concern. This is more fast and realistic in the business world.

- **Structured analysis**: It was the old method of system development and easy to use process of it. It was process oriented system. This integrated with organization structure, management structure, relational database and user interface structure. Security concern in structured analysis has necessity function of corporate organization. Life cycle of software development has proper process of implementation which is also known as levels of data flow analysis.

- **Modeling**: many ready models of systems are available on internet and in open source database but developer have to verify about its security concern and check what kind of structural process build with security related function and also check what kind of plug-in need to the system development. UML is useful to improve the analysis methods; Unified modeling language has different concern about object oriented system. Modeling defined specific use of system structure of organization and it mainly focus on target to achieve from the process flow.

- **Waterfall model**: this software is very adaptive in nature. Like an flow of water system development moves from identifying purpose, form blueprint of
it, implementation and testing through verification of its working flow and provide support for maintenance. This is natural flow of structure over network. In modern time many organization has adopted the method of waterfall model which need to modify existing system of organization structure. Any project in organization form with design phase but leave the real need of its development reason. in such cases waterfall model play an important role to fill the gap of needed function and structure between information system, security system and management. Waterfalls cover the entire objective on each phase of structure and complete the need of software devolvement. Once its start using in real time system developer cannot take it back till the last phase of its process of testing. It’s based on predictive concern but its scale of structure and acceptance is high so there will be no error possibility. It’s useful to cover the gap between existing software system and needed tools to improve the business process structure with use of waterfall model.

- **Ad Hoc structured**: this use for specific reason only. This model will never applicable in some other software system. For one project it needs wide planning and implementation entirely for one purpose with ad Hoc structured. With no other system it can compromise for combinational work.

- **Spiral Model**: this model has adaptive approach. And its process flow as planning with inward and continue till proceed with outward which desired from the system. This model use till project completion process and will continue till it need to complete the flow related the system software development process of life cycle.

- **Rapid application development**: this tool use to facilitate the system for software development with minimum time span. And help to develop new model out it process based on the requirement of business organization.

- **Prototype**: it is the model of support to the system designer to create system and add information system that’s flexible in process and building innovative software through the use of iterative process. It’s useful to quantify the process. It reduces the cost and save time of development. This model always provide chance to improve the software system.
• Microsoft solution framework: It’s based on the series of models added together to solve the purpose of object to develop it. It base on the process of planning and object oriented design process.