CHAPTER - IX
INFORMATION AND TECHNOLOGY ACT - 2000 AND OTHER MEASURES FOR CONTROLLING / SUPERVISING FINANCES

Introduction

Most information security managers in DCCBs have a relatively clear understanding of their role in the Bank for safeguarding the finances. In brief, it is their task to help to:

1) Ensure the availability of valid information about finances when users need it to run the business.
2) Protect the confidentiality of sensitive Bank financial information.
3) Protect the privacy of users in the finance related matters.
4) Protect information assets from unauthorized modification leading to cash manipulation.
5) Ensure the ability of the Bank to continue finance related operation in the event of a disaster.

In summary, while safeguarding the finances, the task of the Information Security Officers and the professionals on DCCBs staff usually:

6) Advice bank management on the policies and procedures needed to protect Bank information assets (including information itself and the ability to process it).
7) Develop procedure and controls in conformity of policy.
8) Assist in implementing procedures, controls and information security tools and devices.
9) Assist in ensuring that managers and employees are aware of their responsibilities to protect information assets.
10) Plan for recovery and continuity of the Bank business in this event of disaster.

11) Advise management in the event of special requirements.

12) Advise users and systems developers on the implementation of controls for sensitive applications.

13) Assist in solving problems concerning information security.

The measures for the security of finance or finance related information:

Keeping the finance and its related information secret is an important task before the Bank. They have to face the problem that how can information on computer based systems be protected against the breaches of security. There are possibilities of illicit computer or financial books uses such as hacking, illegal access, forgery, dental of legitimate access, etc. So, the information officers must be aware of the measures for the security of information. They can be given as follows:

1) **Screening:-**
   
   Using appropriate wiring to screen off radio wave emission from computers, VDUs networks, etc. which can be picked-up by sensing equipment.

2) **Encryption:-**
   
   Scrambling the original signal so it becomes meaningless to an interceptor, particularly relevant for the transmission of data over long distances.

3) **Passwords:-**
   
   To substantiate legitimate access to a system and which can be set by the system’s operators.
4) **Data Protection:-**
   To ensure the integrity of data and to offset the effects of accidental loss or destruction.

5) **Security Policy:-**
   To set, react, write, delete and append access to data files. This may also include setting-logging procedures to track user’s behavior in the system automatically.

**Objectives of Information Security and Control:-**
(i) To prevent malicious damage.
(ii) To prevent accidental damage.
(iii) To limit or reduce the impact of deletions.
(iv) To prevent unauthorized access to location.
(v) To protect the integrity and confidentiality of data.
(vi) To provide for disaster recovery system.

**DCCBs' Information Security and Control (ISC):-**
The essences of ISC are as discussed ahead

(i) **Integrity:-**
A system is considered to be having integrity if it performs, as intended. System designers attempt to develop a system that has functional integrity, which means the ability to continue operating even when one or more components do not function, e.g. distributed functioning network that continues to function, after one of its processors becomes inoperative.
(ii) **Audit-ability:-**

Means that it is relatively easy for someone to examine verify or demonstrate the performance of a system. People who are independent of the system organization, such as internal and external auditors, conduct the audit. A system to be auditable, it must meet the tests of accountability and visibility. Accountability is that responsibility for each event occurring within the system must be traceable to a single individual. Visibility means that unacceptable performance is called to the attention of the system managers. E.g. A computer programme is auditable when the systems analyst and programmer provide a complete programme documentation package and the programme should include the necessary checks for errors.

(iii) **Controllability:-**

It permits management to exercise a directing or constraining influence over the behavior, use and content of the system. One technique for achieving system controllability is to divide the system into subsystems that handle separate transactions. A breach of integrity in one subsystem does not comprise the entire subsystem e.g. one subsystem say opening accounts in a bank controls the second subsystem process i.e. withdrawals. The first subsystem controls the second to prevent unauthorized manipulations of funds, such as someone’s opening a fictitious account for transfer to other accounts.

**Environment for information security:-**

The information security function, as a distinct entity, is originated in the mainframe environment of the 1960s with the introduction of network access to mainframe computers. The initial protective mechanisms and security controls were oriented to this
centralized systems architecture until late in the 1980s. In fact, in many Banks, this orientation remains. As a result, most information security organizations reside within the management information division.

Till 1970s, it was realized by some information security practitioners that information was scattered throughout the Bank on various Medias. That recognition led to a brief struggle among the Bank security department, the internal audit department and the management information system division for ownership of the information security group.

The first shock to this centralized viewpoint came with the advent of minicomputers and distributed computing. Suddenly, information security professionals were faced with computers that were outside the “glass house” and yet connected to networks that reached the mainframe. Frequently, the tools to implement distributed security controls were not available and Banks were reluctant to hire additional security staff for remote operations.

Next came the shock of decentralization of the management information system function as many Banks pushed control of Information Security (IS) resources out to the business units which they served and as many users acquire personal computers that were connected to corporate networks. In the early and mid-1980s, this friend was compounded by the mounting acquisition and divestiture activity of many Banks as they restructured their businesses. This rapid movement of “parts of Banks” created problems for management information system and near-impossible challenges for information security.
Two more trends surfaced in the late 1980s to compound the problem. One trend was that many Banks turned to outsourcing of information systems to reduce their costs. This resulted in the information security group either being “sold” to the outsourcing supplier or remaining in the Bank as a part of substantially diminished management information system function.

Other trend was that Banks formed close operating relationships with both suppliers and customers to improve efficiency of operation and meet competitive threats. In the process, they opened their systems and networks to access by financiers and customers, whose information security procedures could not be controlled by the Bank that established the relationship.

As if all these were not enough, two other technological /marked developments have increased the vulnerability of Bank information. First, portable computers in a variety of forms are carrying Bank information into the world at large. Second, one way or another, most Bank networks are or will soon be connected to the Internet, without stringent means of protection, can allow any clever computer hacker to penetrate Bank computers.

In this rapidly changing environment, information security managers must find a way to convince their Bank executives that business operations may depend on the quality of their information security.
Salient ingredients of Information Security and Control

'Security' may be defined as the protection of both physical and conceptual resources from natural and human hazards. The manager exercises control over the system to ensure that it performs as intended. If the system performance is to be maintained, then the system must be kept secure from disruptive influences.

'Security' concerns in information and technology have been receiving highest attention both from designers and the government. Since, shift is from paper to electronic media and transactions happen from remote and unknown locations, ascertaining the genuine nature of commercial transaction is difficult. Therefore, information security and control is very important.

A strong information technology security programme especially for banking funds cover a number of key areas, include:

- Computer Security:-
- Accountability:-
- Audit ability:-
- System Integrity:-
- Computer Viruses:-
- Internet Connectivity:-
- Access Restrictions:-
- Embezzlement:-
- Outside computer services:-
- Physical Access to Servers:-
- Physical Protection of the Computer:-
- Data Backup:-
- Cost Effectiveness:-  
- Ease of Implementation:-  
- Policy Compliance:-  

Unfortunately almost all the DCCBs have made a little or no concern to these requirements. The forth coming text deals with this aspect

**Computer Security:-**

The rapid advance of computer technology in recent years has given the banking industry another security concern. Illegal entry into computer of a DCCB can greatly threaten the organization’s financial stability. Fires, natural disasters, and hardware theft can result in damaged or irretrievably lost data.

Each banking operation should regularly conduct a complete risk assessment of all computer systems to uncover specific areas of vulnerability. This is an assessment of the risk associated with the loss of each and all systems as well as all data stored on those systems. This assessment should be repeated annually or as new systems are brought online and legacy systems are replaced.

**Accountability:-**

The structure and resources of DCCB usually require that one person carry the responsibility for overall computer system security. In many DCCBs this is either the controller or the officer in-charge management information systems (MIS). However, every one must be held accountable for protecting the information resources of the DCCB
and the MSCB. Sharing system or file access passwords or providing other information that could allow unauthorized access to a DCCBs' systems is equivalent to Bank sabotage or theft. It becomes important, therefore, to limit access to information and systems to those users who require such access to perform their assigned duties.

**Audit ability:**

It is the responsibility of the designated systems security officer of the DCCB to maintain awareness of when users are accessing information, what they are accessing or modifying, and when and how unauthorized attempts to access a system are being made.

The use of unique passwords is one acceptable method of authorizing use and protecting computer data. When a DCCB uses passwords, it should strongly encourage employees to avoid writing them down. Any master list of passwords - whether on paper or electronic - should be protected from unauthorized access. Some DCCBs choose to change passwords at random; some computer systems prompt for new passwords at regular intervals. Passwords of employees who have left or been transferred or terminated may be held in reserve for a suitable length of time before being reissued to other employees; some DCCBs permanently delete the passwords of such persons from the systems.

In order to maintain an audit trace and monitor system usage, system administrators in conjunction with the security officer in the DCCB should activate access, violation, and modification logs that track password use. Access logs provide an electronic record of each attempt to log on to a system. Violation logs record who attempted to
violates system or file - level security, and modification logs records user information on all files that have been modified. In some systems, it is possible to have such logs activate an alarm when data gathered in the log fall outside established parameters. Such notification allows the system administrator the opportunity to locate the source of the potential security risk.

**System Integrity:**

There is not a security plan or system for computers that is 100 percent foolproof. In fact, many information technology (IT) managers say, "You do the best you can. After that, if someone really wants to get into a system, they will get in." Unfortunately, this is true. Since such access can happen from within a DCCB or from the outside, it is important to take measures to prevent "hacking" into a system on both fronts. It is the responsibility of the appointed systems security officer to perform due diligence as it relates to system integrity, keeping the system continuously operational without data loss or security incident.

The level of security available on a particular system in most cases begins with the operating system. For example, Microsoft's Windows 95 and Windows 98 are desktop operating systems designed primarily for home and small-business computer users; they offer less security than Windows NT and Novell Netware, which are network operating systems.

**Computer Viruses:**

Computer viruses are destructive computer programmes that can "infect" a computer, damage data files, system files, and
applications. Viruses can replicate themselves and can be transmitted as hidden files or programmes from one computer to another. Viruses are most often transmitted when users carry a floppy disk from computer to computer, copying files to and from the disk without considering whether or not they might contain a computer virus. An infected disk may invisibly transmit the virus to each computer that reads the disk. This in turn infects one computer after another. The second and much more effective (and malicious) way viruses are spread is over the Internet. Internet mail attachments are notorious for carrying computer viruses. These programs are attached to e-mail messages and then sent to numerous users. The unsuspecting user then opens the mail and carelessly infects the computer with a virus.

The most effective way to prevent the spread of computer viruses is to use a computer programme that "inoculates" a machine and its data against the threat of viruses. These programs work as virus shields, scanning files for known computer viruses as they are opened or run. If a virus is detected, it is immediately cleaned from the system. Additionally, these programmes can be set up to periodically scan the entire computer for viruses. Virus protection programme are extremely effective when installed on a server and used in a local area network (LAN). In this situation, any data that is stored on the server can be scanned and cleaned on a regular basis. Because new "strains" of computer viruses are constantly being developed and circulated, virus-protection software should be updated regularly to ensure the best protection possible. Some DCCBs now make such software updates available for easy downloading form their Web sites.
Internet Connectivity:-

When computers have access to the Internet as well as corporate and local area network, it is important to protect data from unauthorized distribution over the Internet. It is especially critical to control Internet access centrally in any DCCB where computers are connected to the DCCB LAN and to the Internet via a modem. Anytime there is a modem on a PC, there is the possibility for unauthorized transmission of data from the network, out of the DCCB, via the modem. It is more secure to provide Internet access via the network so that a fire-wall can be put in place to protect the DCCBs data and systems. Firewalls are communications filters that allow only authorized access and data transmission to and from a network.

Access Restrictions:-

The more people that have access to a computer, the greater the possibility for compromised security. Implementing certain access restrictions can help to maintain system integrity.

One type of restricted access involves the creation of different levels of authorization for access to different levels of information. Such systems limit the information available to employees to only those areas necessary for the performance of their jobs. Front desk staff, for example, would be limited to computer access relating to the check-in and check-out functions only.

In some DCCBs, it may be necessary to limit the time periods during which computers may be accessed. This can be managed through the user rights and privileges aspect of a network operating system. For example, users may be granted access to the network only
between 9:00 a.m. and 5:00 p.m. This prevents access to data when there is no network administrator available to monitor data activity.

**Embezzlement:**

Embezzlement is a major crime against which computers should be protected. With a little knowledge of programming, it is fairly easy to set up dummy accounts in order to embezzle money. Funds may be directed to such accounts for long periods of time before being detected. The use of passwords and restricted levels of access help to safeguard a DCCBs' assets, but it is not possible to completely eliminate the potential for someone to bypass these safeguards. Security systems can only make it difficult for unauthorized persons to gain access to the computer; authorized personnel may be in positions of authority that allow them access to important restricted information which they use for illegitimate purposes.

There are a number of ways to reduce the potential for embezzlement by computer. Some involve the same procedures used for preventing embezzlement of any sort. For example, there should be a separation of duties. The computer programmer should not also be the computer operator. This separation of duties prevents the programmer from building loopholes into the programme to permit access later for personal profit. Also, the computerized check writing operation should be separated from the department that authorizes checks, in order to keep false data from resulting in actual cash payments. A single individual should not be able to generate a payment. Some DCCBs use a mandatory vacation policy to ensure that every employee's work - including that of potential embezzlers with
access to the computer – is periodically reviewed by someone else (that is, the employee who substitutes for the vacationing employee).

Outside computer services:-

Perhaps somewhat surprisingly, protection from computer embezzlement and fraud may sometimes be enhanced through the use of outside computer services. Although this practice involves revealing internal information to persons outside the organization, the people seeing it will generally have little personal use for it – especially if the service is well organized and conscious of the security requirements of its clients. Employees within outside computer services seldom have the opportunity to gain the familiarity with a DCC that is needed to effectively embezzle its assets. This is especially true when the DCCB assigns different computer responsibilities to more than one outside computer service. Contrast this with the situation in which corrupt or potentially corrupt internal employees have such detailed knowledge of the workings of the DCCB that they are relatively well equipped to embezzle in ways that are hard to detect.

Of course, care should be taken in selecting an outside service. A DCCB choosing a service should ensure that the service has an effective internal security programme. This involves not only protecting the confidentiality of the information entrusted to the service, but also taking adequate precautions against hazards such as fire, flood, vandalism, civil disturbances, power blackouts, and more. The service also should be financially sound; services that are not may be more susceptible to the temptation to misuse their positions of trust. Also, there is the potential for records and documents to be tied up indefinitely if the service goes bankrupt.
Physical Access to Servers:-

The server room or main computer room in a DCCB should be secured in a separate area from other operations, protected by adequate locks and double-door entry. All movement of personnel into the area should be controlled, and access should be granted only to those who work with the network. A log should be maintained in computer operating areas detailing any stoppages and any resulting problems. Such records should be maintained and reviewed regularly by supervisory personnel.

Physical Protection of the Computer:6

Computer security involves more than protecting against fraud or vandalism. The computer itself should be maintained and protected from numerous hazards that could temporarily or permanently incapacitate it.

The greatest danger is fire. Compute rooms should be constructed of fire-proof or fire-resistant materials. Sprinkler systems may be useful, although flooding is not good for computers either. Systems that use special gases that rapidly extinguish fires are available, but they are expensive to maintain. Review the local fire code requirements; some jurisdictions mandate water sprinkler systems in addition to or in place of chemical systems. Employees should be trained in how to react quickly and effectively to a fire in the compute room or a fire that may threaten the computer room. Because simple overheating can also be a problem, computer rooms are often air conditioned.
DCCBs also should take measures to protect against power failures that may disrupt computer functions. One strategy is to route all computer equipment through an uninterrupted power supply (UPS) unit. Common IT problems such as electrical outages should have recovery procedures detailed in a disaster hand-book. These procedures should provide step-by-step instructions on how to maintain critical systems using back-up power facilities and how to recover any transactions that were in process when the outage occurred.

Computer equipment, although increasingly affordable, is still coveted by many unscrupulous individuals. It is therefore paramount that desktop equipment be secured in place to prevent theft. Anti-theft systems include those that can be used to mount equipment to a base that is then secured to a desk or the floor, cable and lock systems, and systems that use fiber-optic cable and an integrated alarm system.

Finally, every DCCB should develop a comprehensive disaster recovery plan that includes procedures for recovery from both natural disasters and premeditated, malicious attacks on critical information systems.

**Data Backup:-**

It is most important that all critical data on a DCCBs' network be backed up each day. Additionally, critical report information should be printed at regular intervals in case of emergency or system outage. For instance, room occupancy and guest information should be printed regularly (for each shift) so that room status can be determined in the event of the system going down.
Physical backup on tape, high-capacity disk, or recordable CD/DVD should be performed daily and stored off-site in the event of fire or theft of system equipment or data. In some instances, corporate policies will govern backup procedures and the storage of backup media. Otherwise, each DCCB should develop adequate procedures that meet the needs of that DCCB.

**Cost Effectiveness:**

While cost effectiveness is important, it also is important to gain the commitment from senior management to invest in the appropriate level of resources to protect the information systems of the DCCB. In all cases, the level of resources allocated to securing data should be directly proportional to the value of the data to the bank. Systems in computer labs for training, for example, may hold data that can be easily replaced or reinstalled; therefore, data security there is not a high priority. However, DCCB with irreplaceable proprietary business information might use data encryption on all file transmissions, implement redundant data storage, and manage all security procedures closely; the financial life of the organization may depend upon it.

**Ease of Implementation:**

Data and system security should be relatively easy to implement. An overly complex system may be underutilized or incorrectly setup because it is too difficult to work with, thereby compromising system integrity. A system should be flexible enough to assign access to system resources and information as needed without using extensive IT staff resources. Frequently, network operating systems allow system administrators to grant company-wide access by user type. Many DCCBs management systems allow for the
assignment of user rights by job function: the front office manager would have additional rights to those granted to the reservationists or the guest services representative that works the front desk. These are easily implemented user parameters that are controlled by the application or by the system software.

Policy Compliance:

In addition to a well-designed security plan, complete with policies and procedures related to accountability, audit ability, cost effectiveness, and ease of implementation, IT managers must be concerned with general safeguards against unauthorized access to data and continuous system operation.

Additional policies and procedures may be set to ensure data security. Password protection of system and file access is a classic example of a basic security parameter. However, once a password is revealed, it is useless as a security parameter. It is therefore important to implement policy associated with password management. The severity of the policy depends on the needs of the Bank. For example, requiring users to change their password daily on a saving or current account system would be counterproductive. However, implementing the same policy in the employees’ salary accounting might be considered prudent.

Computer security involves many aspects of the computer system. It is important that IT managers or the responsible party at the DCCB consider all aspects of computer security. Additionally, security managers should communicate to other DCCB employees the importance of security and their role in the effectiveness of overall security of the DCCBs’ information systems.
Information and Technology act – 2000

The important objectives of Information and Technology act – 2000 are as follows:

(i) To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper based methods of communication.

(ii) To give legal recognition to Digital Structure for authentication of any information or matter which requires authentication under any law:

(iii) To facilitate electronic filing of documents with Government departments.

(iv) To facilitate electronic storage of data.

(v) To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.

(vi) To give legal recognition for keeping books of accounts by Bankers in electronic form.

(vii) To amend the Indian Penal Code, the Indian Evidence Act – 1872, the Banker’s Book Evidence Act – 1891 and the Reserve Bank of India Act – 1934.
Scope of the Act:-

The Act shall extend to the whole of India and, unless otherwise provided in the Act, it applies also to any offence or contravention there under committed outside India by any person.

The Act however, shall not apply to the following:
(i) A negotiable instrument as defined in section - 13 of the Negotiable Instrument Act - 1881;
(ii) A power-of-attorney as defined in section 1 A of the Powers-of-Attorney Act - 1882.

II

SALIENT MANAGEMENT ISSUES IN MIS OF DCCB CONCERNING TO SECURITY/SMOOTH WORKING

Ethical and social dimensions of Information Technology (IT):-

Now we are in the midst of an information revolution in which information technology has dramatically magnified our ability to acquire, manipulate, store and communicate information. We have electronic tools to retrieve and communicate information in seconds to any person, in any place and at any time of the day. We can now communicate easily, work co-operatively, share resources and make dimensions all electronically. It has now become possible to engage in ethical or unethical business practices electronically anywhere in the world. That's why, it is important to understand the ethical dimensions of working in Banking business and using information technology.
The following figure illustrates several important aspects of the ethical and social dimensions of information technology:

![Diagram showing the relationship between Social Solutions, Employment, Working Conditions, Health, Privacy, Individuality, and Crime.]

It emphasizes that the use of information technology in DCCB has major impacts on society. It raises serious ethical considerations in areas like privacy, crime, and health, working conditions, employment and the search for social solutions through information technology.

The way to understand the ethical dimensions of information technology is to consider the basic issue that arise from its use to gather, process, store and distribute information. It is seen that information systems control people or their intellectual capital. For e.g. People can lose information without compensation and without their permission. People can also be denied access to information or be exposed to erroneous information. Mason proposes the development of a new social contract where information technology will help to ensure everyone’s right to fulfill his or her human potential.
1) **Information Technology and Employment:-**
The impact of information technology on employment is a major ethical concern. It is directly related to the user of computers to achieve automation. Information technology has created new jobs and increased productivity. In the same way, there is a significant reduction in some types of job opportunities. Information technology has created a host of new job opportunities for the manufacture, sale and maintenance of computer hardware and software and for other information system services. Many new jobs have been created in computer using organizations. For e.g. systems analysts, computer programmer and computer operators etc.8

2) **Information Technology and Individuality:-**
There is negative effect of information technology on the individuality of people. Computer-based systems are criticized as impersonal systems that dehumanize and depersonalize activities which have been computerized. It is because they eliminate the human relationships present in non-computer systems. Another aspect of loss of individuality is the regimentation of the individual that seems to be required by some computer-based systems. These systems are not flexible. They demand strict adherence to detailed procedures if the system is to work.

3) **Information Technology and Working Conditions:-**
Information Technology has eliminated monotonous or obnoxious tasks in the office and the factory. This allows people to concentrate on more challenging and interesting assignments. It upgrades the skill level of the work to be performed. It creates
challenging jobs requiring highly developed skills in the computer industry and within computer using organizations. Thus, it can be said that information technology can be used to upgrade the quality of work because it can upgrade the quality of working conditions and the content of work activities. Of course, it must be remembered that some jobs created by information technology, data entry are quite repetitive and routine. The work with the computers is sometimes a work where a worker is forced to work like a machine instead of a like a skilled craftsperson.

4) Privacy Issues:-
Information Technology makes it technically and economically feasible to collect, store, integrate, interchange and retrieve data and information quickly and easily. This has an important beneficial effect on the efficiency and effectiveness of computer-based information systems. However, the power of information technology to store and retrieve information can have a negative effect on the right to privacy of every individual. For example, confidential e-mail messages by employees are monitored by many companies. Confidential information on individuals contained in centralized computer databases by credit bureaus. Government agencies and private business firms have been stolen or misused. This results in the invasion of privacy, fraud and other injustices. The unauthorized use of such information has seriously damaged the privacy of individuals. Errors in such databases could seriously hurt the standing or reputation of an individual.
5) **Computer Crime:**

Computer crime is a growing threat caused by the criminal or irresponsible actions of small minority computer professionals and end users how are taking advantages of the widespread use of computers and information technology in our society. Thus, it presents a major challenge to the ethical use of information technology. Computer crime also possesses serious threats to the security of computer-based information systems and makes the development of effective control methods as a top priority.

6) **Health Issues:**

The use of information technology in the workplace raises a variety of health issues. Heavy use of computers is reportedly causing health problems like job stress, damaged arm and neck muscles, eyestrain, radiation exposure and even death by computer-caused accidents.

7) **Social Solutions:**

It would be good to emphasis that information technology can have many beneficial effects on society. We can use information technology to solve human and social problems from societal solutions such as medical diagnosis, computer-assisted instruction, Government programme planning, environmental quality control and law enforcement. For example, computers can be used to help to diagnose an illness, prescribe necessary treatment and monitor the progress of hospital patients. Computers are also used for the programme planning of many Government agencies in such areas as urban planning population density and land use studies, highway planning and urban transit studies. Thus, such applications illustrate that
information technology can be used to help in solving the problems of society.

DCCBs affiliated to MSCB are themselves concern for the interlinking to act effectively.

Information technology is an important tool in making this transformation and in designing the state Cooperative Banking. One can expect to see Bank's rapidly moving operations to different parts of the state to take an advantage of special competencies and disparities in wage rates. Even a one-person Bank can have worldwide operations through the Internet. All the information technology design variables that focus on communications are available to help, manage and co-ordinate the state cooperative.

A state co-operation needs information to co-ordinate and control its diverse co-operative businesses. Reporting and early warning systems are very important in this environment. Systems that summaries loans/deposit data and process accounting information are necessary but they only reflect what has happened in the past. These systems represent traditional uses of information technology for reporting and control.

Technology offers many more active tools to help and manage the business. Co-ordination is a major problem for the MSCB. Information technology provides a number of approaches for improving communications and co-ordination. To manage informal systems for MSCB is a problem before the managers.

Roche presents a number of strategies for managing information technology in a global environment. They are as follows:
1) **Concentrate on inter DCCB linkages:**
The strategy of creating linkages with financiers (lenders,
depositors) and customers can be extremely effective to MSCB.
It can also be very difficult to set up these linkages because of
differing telecommunications' capabilities in different regions.
In some district, phone systems do not work well and
transmitting data over them is probably not viable. Other
regions like Mumbai have an extremely well developed
infrastructure for business communication. The Internet is one
solution for quickly establishing these linkages.

2) **Establish systems development skills in DCCBs/MSCB:-**
There are problems managing information development
projects when all participants are from the same Bank and work
in the same location. Coordinating state level project teams
present an event greater challenge. Language and distance make
them difficult to co-ordinate. It needs personnel skills. Lack of
personnel skills can be a major impediment in developing state
level systems. In the same way, all the DCCBs do not have
educational programmes to prepare individuals for system
analysis for programming jobs.

3) **Build an Infrastructure:-**
Justifying expenditure on infrastructure can also be extremely
difficult. Infrastructure is the part of technology that does not
have an immediate benefit. The economic criteria has suggested
not to undertake the development of the network. However, the
MSCB went ahead and found that the new information
technology provided a number of benefits that were hard to
quantity. Basically, with this network, the MSCB could plug in
any application to the network and offer it any place in the world it did business.

4) **Take advantage of liberalized electronic communications**: The trend towards deregulation in India is also replacing monopoly. Government has separated its Telecom from the PTT and established it as a quasi public organization. In the past two decades, Indian Telecom has replaced an outmoded phone system and added a mass-market communications network called the Minutely System. It is also a leader in providing packet-switched data communications through transact. Such changes facilitate the development of the MSCB communications’ networks, which is essential for managing DCCB throughout the states by MSCB.

5) **Strive for uniform data**: One of the major problems in sharing data is to identify it. It is said that a large computer vendor once looked at its logistic systems and found that “ship date” meant six or seven different things depending on the system involved. In one system, it might be the promised ship date and in another date, the item left the loading dock. To obtain economies of scale from sharing data and systems, the DCCBs must have a common vocabulary of terms and definitions.

6) **Develop guidelines for shared versus local systems**: MSCB needs to develop guidelines for when a system should be shared and when a local autonomous system is more appropriate. The advantages of shared systems are economies of scale and the ability to share data. The problem with shared
systems is that they tend to become very large and complex. Individual locations and users have special needs that must be incorporated into the system. As the number of exceptions increase, the system becomes more cumbersome and difficult to programme.

The advantage of a local system is that it can be developed quickly in response to a local condition. If it later becomes necessary to co-ordinate this system with other applications, special interfaces will have to be created.

There are no firm guidelines for making this kind of decision. Firms have success and failure with both approaches. Systems development in an international environment leads to this problem. Management has to recognize that the problem exists and compare the alternative of local versus global or shared systems.

Management Control over Information Technology:-

Information Technology can provide novel ways to control the organization, making possible new organizational structures and alliances with external firms. The firms having extensive outsourcing face problems of control and communications. Managerial control and co-ordination are closely related.

One of the fundamental rules of management in an organization is control. Process control offers useful models for thinking about control in general.
The following figure shows a typical control system:

In this system, a sensor determines actual conditions and a comparison device compares the standard with what actually exists. If the difference between reality and the standard is too great, the comparison device sends a signal to take an action. The action taken, in turn, affects the sensor and standard and the cycle continues until the comparison device finds an agreement between sensor and standard stops signaling for an action.⁹

In an organization, we can apply the same concepts. Managers have a notion of a standard and they must become aware of deviations from the standard with the help of some given indicator deviates from the standard, management must take action to bring the organization back into control.

The following figure shows some of the tools available to managers at different levels for controlling the organizations.

Top management can create control through the structure of the organization. For example, management can decide do decentralize and to have local managers responsible for comparing their
performance with the goals that the managers set for the year. As an alternative, top management can opt for a high degree of centralization. So it can set a policy and review all decisions.

The discussions of the T-Form organization suggest that in the future, management will have a more difficult time using traditional methods such as structure for control. Hierarchical structures are in retreat and managers will have to trust subordinates and come up with new ways to exercise their responsibility for control.

Top management also exerts to control a reward structure. Several brokerage firms suffered control breakdowns, partially, we suspect, because of a reward structure encouraging heavy risk tasking in bond trading. The firms paid bond traders very large bonuses based on performance because bond trading is highly competitive among firms. More than one firm found it lost well over $100 million in a few weeks when the market turned. There was a highly motivating reward system and almost no managerial control over the traders. Two banks recently found losses of over one billion dollars in unauthorized trading, forcing one bank into a merger.

One form of managerial control that is used frequently and probably could have helped ameliorate the bond trader problem is the management committee. For many years, banks have employed loan review committees. The lending officer has a certain limit which he or she can approve on a loan. Any loan larger that the limit must be discussed and ultimately approved by the committee. The committee serves as a review and control role in the firm.

The most frequent middle management control device is the budget. Many managers in the organization received periodic budget
reports that inform them of actual versus targeted performance. Budgets are extremely important tools for controlling expenditures.\textsuperscript{10}

Middle managers are also expected to exert direct supervision over their subordinates, though more remote work makes this difficult. When in doubt, they can refer problems up through a managerial hierarchy. The entire structure of management serves to control the organization and keep it on course. Middle managers can also establish review committees to foster greater control.

At the lowest levels of management, we find procedures describing how operations should be done. Procedures were particularly evident in paperwork transactions processing departments. If one visited an accounts payable operation, it was possible to see clerks who carefully looked up each bill that the firm received and to find the purchase order that authorized the purchase. The clerk saw that the goals or services purchased actually arrived and delivery was satisfactory. Then the clerk authorized the payable and put all the documents relating to the payment into a voucher which was filed for a number of years.

This kind of manual accounts payable operation is rapidly vanishing which creates new control problems for the organization. Consider – ‘Chrysler’s Pay’ as Built programme where it calculates, what it owes suppliers based on each day’s production and sends on electronic payment. How do Chrysler and its suppliers know that the calculations and payment are correct? At some point in time, the number of components shipped to Chrysler should make the payments but verifying these transactions could be a formidable task.
Regular routine audits help to establish control by showing that control is important and by sending the message that there is a form of quality control over all the firm’s procedures or at least those affecting financial statements. Lower level managers also have direct supervision responsibilities. They too can make use of the managerial hierarchy to obtain approvals or additional guidance.

Information and Control:-

One contribution of information systems is to strengthen control systems. A manager needs information about the deviation of actual from standard or targeted performance. Computerized budget systems help managers to identify expectations and take an action. Execute information systems monitor critical indicators for management. Senior management may be able to take immediate action if sales are falling below projections. Managers may alter production schedules, emphasize different products and / or begin to reduce expenditures.

Although information systems can help to improve managerial control, they create a tremendous control over the problem themselves. Information systems are very complex. For example, it is likely that no one person understands everything about a large system like ‘SABRE’. So although managers do not necessarily understand the technology, they are often responsible for seeing that information systems are under control.

Computerization in Co-operative Banks For Better MIS: 11

On Threshold of Computerization:

The Banking Industry in India is in the process of switching over to Computerization in regard to its day to day operation and
laying greater thrust on the Management information Systems. In fact, this process should have been started in Seventies when the Banks were nationalized. There was no urge on the part of Management to take to Computerization on the stock argument that mechanization will create unemployment. The Trade Unions were also opposed for the same reason with added fervour. This attitude was due partly to ignorance of the mechanism of computers and partly to inaction on the part of Executives to update their expertise instead of continuing the outmoded practices and procedures. This trend is still continuing and there is no desire on the part of Officers and Executives to apply their energies in understanding and assimilating the modern Techniques in computerization and its organization. The transition to computerization is, therefore, going to be a tussle between the old ideology and new technology.

**What is Computer?**

A computer is an all purpose calculating machine. It performs all mathematical calculations very speedily. It also does statistical work, namely classification and tabulation of data and desired. It can also merge, delete, compare and do other diverse mathematical and other operations as required.

The main advantage of a computer is that it can store data in its memory units indefinitely. These memory units are in the form of magnetic tapes of a Tap Recorder or Floppy discs (similar to long playing records but in different sizes). This data can be recalled at any time. It can be erased, updated, modified as desired. These memory devices are in a very portable form and can be stored in special cabinets requiring smaller space.
Ready and quick calculation, recording, storage and recalling of data are main characteristics which are not present in any ordinary machine.

The data base-information which we want to access is fed into the machine through input device. It is then stored into Memory unit so that it can be recalled and connected to at any time to the central Processing Unit (CPU) for processing the data. After it is processed, the resulting information is printed through Output unit in a language of the user.

Present profile of Co-operative banking:¹²

Co-operative Banks are growing in number as well as in Resources. The norms of viability as laid down in the Madhavadas Committee are absolutely out of date. There is a need for further in-depth study of viability. The Inflationary conditions are playing havoc with the result that the purchasing power of Rupee has touched a low of 10 paisa or even lower. The comparison with previous years is meaningless. There is a need for preparing a new base for cost of living index.

With growth in numbers, the standards of operational efficiency and productivity have suffered. Even the leading District Co-operative Banks are not exception. The same outdated procedures, which are nearly 50 years old, are being followed. It is really a pitiable sight to see that the clerks are handling fat and weighty ledgers. There is no switch over to loose leaf ledgers. The patent argument is that the changeover to loose leaf will give rise to fraud. The balancing is still
done by physically taking down the balances and totaling them. 90 per cent of the energy of the staff of these DCC banks - of all ranks - is wasted in balancing the books and updating the statistical returns - which are always “out of date”. The balancing of Books is always in arrears - and the accounts are finalized by opening “Difference Account” to give effect to the Double Entry. Comments to the effect that the books are not balanced, the Inter Bank and Inter Branch reconciliation are in arrears and so on. The Statutory Auditors seem to be silent on this feature and their audit reports give a good certificate. How long is this state a “great leap” to the “Twenty-first Century” which is just round the corner? Should we think of mechanization at the stage? Are we still going to stick to the pet arguments of “unemployment” and all that goes along with it?

**Computer: A tool for Management Information System:**

The use of computer with proper and scientific approach will speed up balancing of books, computation of interest, issue of statements of accounts, daily trial balance and periodical statistical returns as required by the Co-operative Department of State Govt. and Reserve Bank. This will naturally leave more time to the staff for monitoring of performance and formulation of policy and plans for development of the Bank. In fact, the routine matters will be entirely taken over by the computer ensuring thorough accuracy, precision economy of space and personnel and speedy disposal. It will be instructive to identify these areas in more detail.

(i) **Management of Cash:**

The Management of cash is a fundamental requirement in a DCCB. Deposits are basically borrowings from customers with an
undertaking to pay them on demand or at a definite future date. The interest payable on Deposits - Savings’ and Time, starts from the date the funds are received. Even though Savings Deposits may give us a breather owing to computation of interest on minimum balance between the 10th and the last day of the month, the Time Deposits, which constitute quite sizeable resources going up to 60 per cent of total deposits are very costly as the interest rate varies from 10 per cent to 12 per cent. It is all the more necessary that surplus funds are very closely invested keeping a very fine margin for the Statutory Cash Liquidity at 3 per cent. The ready availability of the closing financial position through computer, facilitates simultaneous investment of funds in Call/Short Deposits. The manual operations do not allow the ready availability of data thereby resulting in loss of interest on unutilised funds. It is worth while nothing that in good many Co-operative Banks the concept of close and intensive investment of surplus funds is lacking owing to ignorance and also delays owing to manual systems.

(ii) **Credit Management:**

The management of Agricultural credit is another crucial where the computer can work wonders. We can prepare statistical tables covering the following topics by preparing separate modules on floppies or magnetic tapes:

(i) Preparation of Credit Plan for each Co-operative Society, the year setting out the priorities in definite order.
(ii) Monitoring of the Plan every quarter and updating and modifying the targets where necessary.

(iii) Tabulate overdue position of -
(a) Advances based on the quantum of loan and agewise analysis of overdue installments.
(b) Monitoring of loan recovery by team of officers.
(c) Updating of data and review of loans outstanding.

(iv) Review of large advances as also Prior advances on the basis of date processed by computer.

(v) Classification of advances -
Product wise and purpose wise along with periodical review for shifting priorities, if required.

The classification can be done society wise.

(iii) Profile of Deposits:
Similar exercise can be done for the composition of Deposits. This composition can keep track of the source of deposits - whether they are from salary earners, traders, industrial houses, educational/cultural institutions, corporate sector and so on. The break of deposits - Current, savings, time and various saving schemes - branch wise and amount wise can be compiled. These statistics will come in very handy for projecting the flow of deposits area wise.
(iv) **Membership:**

Members of Co-operative constitute the very base of the organization as contributors to the capital structure of the Bank owing to the linkage of Share Capital to lending. Data can be complied giving us a glimpse into the character and type of membership in the area of operation of the Bank. The Management can formulate its policies in the context of its findings and give a meaningful development thrust. The bank at present is operating a reporting system for different purposes rather than introducing an integrated management information system.
References


