INTRODUCTION
(Chapter 1)
CHAPTER ONE
OVERVIEW OF INFORMATION SYSTEM AUDITING

1.1 Introduction:

Technology has always been intertwined with society’s progress but never before, in history, has technology been so visibly linked to improvements in standards of living. Because of technology, our world is developing at a phenomenal speed. The proper exploitation of technology strongly influences business competitiveness, which is no longer a matter of choice but a matter of survival in the market place. Clearly, the application of technology, not just its development, is a key to success in the competitive global economy. In today’s environment of mobile and digital economy (facilitating seamless connection to anyone, anytime and anywhere), enabling technology is one of the determining factors of successful organization. Therefore, control and audit of information technology/systems is becoming an important function in today’s business organization in order to safeguard assets, maintain data integrity and achieve the goal of organization effectively and efficiently.

1.1.1 History of Information System Auditing:

Information System Auditing (IS auditing) began as Electronic Data Process (EDP) Auditing and developed largely as a result of the rise in technology in accounting systems, the need for IS control, and the impact of computers on the ability to perform attestation services. The last few years have been an exciting time in the world of IS auditing as a result of the accounting scandals and increased regulation. IS auditing has had a relatively short yet rich history when compared to auditing as a whole and remains an ever changing field.

The introduction of computer technology into accounting systems changed the way data was stored, retrieved and controlled. It is believed that the first use of a computerized accounting system was at General Electric in 1954. During the time period of 1954 to the mid-1960s, the auditing profession was still auditing around the computer. At this time only mainframe computers were used and few people had the skills and abilities to program computers. This began to change in the mid-1960s with
the introduction of new, smaller and less expensive machines. This increased the use of computers in businesses and with it came the need for auditors to become familiar with EDP concepts in business. Along with the increase in computer use, came the rise of different types of accounting systems. The industry soon realized that they needed to develop their own software and the first of the generalized audit software (GAS) was developed. In 1968, the American Institute of Certified Public Accountants (AICPA) had the Big Eight (now the Big Four) accounting firms participate in the development of EDP auditing. The result of this was the release of Auditing & EDP. The book included how to document EDP audits and examples of how to process internal control reviews.

Around this time EDP auditors formed the Electronic Data Processing Auditors Association (EDPAA). The goal of the association was to produce guidelines, procedures and standards for EDP audits. In 1977, the first edition of Control Objectives was published. This publication is now known as Control Objectives for Information and related Technology (CobiT). CobiT is the set of generally accepted IS control objectives for IS auditors. In 1994, EDPAA changed its name to Information Systems Audit and Control Association (ISACA). The period from the late 1960s through today has seen rapid changes in technology from the microcomputer and networking to the internet and with these changes came some major events that change IS auditing forever.

The formation and rise in popularity of the Internet and E-commerce have had significant influences on the growth of IS audit. The Internet influences the lives of most of the world and is a place of increased business, entertainment and crime. IS auditing helps organizations and individuals on the Internet find security while helping commerce and communications to flourish.

1.1.2 IS Today – A Review:

High-speed information processing has become indispensable to organizations' activities. For example, Control Objectives for Information and Related Technology (CobiT) emphasizes this point and substantiates the need to research, develop, publicize, and promote up-to-date internationally accepted IS control objectives.
From a worldwide perspective, information technology i.e. computer and communication technology processes need to be controlled.

From a historical standpoint, much has been published about need to develop skills in this field. In its 1992 discussion paper, “Minimum Skills Levels in Information Technology for Professional Accountants,” and its 1993 final report, “The Impact of Information Technology on the Accountancy Profession,” the International Federation of Accountants (IFAC) acknowledged the need for better university-level education to address growing IS control concerns and issues. The Institute of Internal Auditors (IIA) 1992 document “Model Curriculum for Information Systems Auditing” was developed to define the knowledge and skills required by internal auditors to be proficient in the information age of the 1990s and beyond. Around the world, reports of white-collar crime, information theft, computer fraud, information abuse, and other information / technology control concerns are being heard more frequently, through the surveys and reports by SANS (SysAdmin, Audit, Network, Security) Institute, U.S. Government Accountability Office (GAO), Federal Bureau of Investigation (FBI), Federal Trade Commission (FTC), Computer Security Institute (CSI), Computer Emergency Response Team (CERT), and others. Organizations are more information dependent and conscious of the pervasive nature of technology across the business enterprise. The increased connectivity and availability of systems and open environments have proven to be the lifelines of most business entities. Information and communication technology is used more extensively in all areas of commerce around the world.

Essentially, technology has impacted three significant areas of the business environment: -

It has impacted what can be done in business in terms of information and as a business enabler. It has increased the ability to capture, store, analyze, and process tremendous amounts of data and information, which has increased the empowerment of the business decision maker. Technology has also become a primary enabler to various production and service processes. It has become a critical component to
business processes. There is a residual effect in that the increased use of technology has resulted in increased budgets, increased success and failures, and increased awareness of the need for control.

Technology has significantly impacted the control process. Although control objectives have greatly remained constant, except for some that are technology specific, technology has altered the way in which systems should be controlled. Safeguarding assets, as a control objective, remains the same whether it is done manually or is automated. However, the manner by which the control objective is met is certainly impacted.

Technology has impacted the auditing profession in terms of how audits are performed and the knowledge required to draw conclusions regarding operational or system effectiveness, efficiency and integrity, and reporting integrity. Initially, the impact was focused on dealing with the changed processing environment. As the need for auditors with specialized technology skills grew, so did the IT auditing profession.

1.1.3 IS Audit Course of ICAI: -

Owing to the rapid diffusion of computer technologies and the ease of information accessibility, knowledgeable and well-educated IS auditors are needed to ensure that effective IS controls are in place to maintain data integrity and manage access to information. Globally, private industry, professional associations, and organizations such as International Federation of Information Processing (IFIP), Association of Computing Machinery (ACM), Association of Information Technology Professionals (AITP), Information Systems Security Association (ISSA), and others have recognized the need for more research and guidance. Control-oriented organizations such as the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), IIA, Association of Certified Fraud Examiners (ACFE), and others have issued guidance and instructions and supported studies/research in this area.
Several universities have offered training courses and curriculum in IS auditing. There are number of professional organizations in different countries supporting the professional development of the IS auditor through conducting seminars/conferences, workshops, issuing guidelines for IS auditing, providing professional certification with specific discipline. Some of the courses are Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Governance of Enterprise IT (CGEIT), Certified Computer Professional (CCP), Certified Software Quality Analyst (CSQA), Certified Information Systems Security Professional (CISSP), etc.

In India, to equip the Chartered Accountants with the knowledge of tools and techniques related with computer based information systems auditing the council of Institute of Chartered Accountants of India (ICAI) already established a Committee on Information Technology (CIT) in the year 2000. And the ICAI is conducting the examination for the Post Qualification Course on Information Systems Audit (DISA) for its professionals. The Institute (ICAI) is running the ISA professional training (ISA PT) programme at its different regional / branch offices to handover the training and course materials for the said course. Further, Institute conducts examinations of ISA ET (Eligibility Test) and ISA AT (Assessment Test) in order to check the competency of its professionals and provide the certificate of Post Qualification Course on Information Systems Audit to successful candidates. The table 1.1 in next page lists the revised course modules, percentage of questions that are applicable for the ISA ET & AT effective from January 2006.

<table>
<thead>
<tr>
<th>Module</th>
<th>Module Title</th>
<th>%Q’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Technology Infrastructure</td>
<td>10%</td>
</tr>
<tr>
<td>2</td>
<td>Communication &amp; Networking Technology</td>
<td>22%</td>
</tr>
<tr>
<td>3</td>
<td>Protecting Information Assets</td>
<td>22%</td>
</tr>
<tr>
<td>4</td>
<td>Systems Development. Life Cycle &amp; Application Details</td>
<td>20%</td>
</tr>
<tr>
<td>5</td>
<td>Business Continuity Planning</td>
<td>8%</td>
</tr>
<tr>
<td>6</td>
<td>Information Systems Organisation &amp; Management</td>
<td>8%</td>
</tr>
<tr>
<td>7</td>
<td>Information Systems Control &amp; Audit Process</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: www.cit.icai.org
1.1.4 Definition of Terms and Concepts:

1.1.4.1 Effectiveness:

In human-computer interaction, effectiveness is defined as "the accuracy and completeness of users' tasks while using a system". Effectiveness means accomplishment of the objective i.e. setting right targets to achieve an overall goal (doing "right" things). Effectiveness differs from efficiency as efficiency is nothing but doing things in most economical way (i.e. accomplishment of objective in shortest time with minimum resources).

1.1.4.2 Information:

Meaningful data i.e. result achieved from the processing of data through the computer or other means. For example, suppose we are using juice maker to process the fruits in order to obtain the juice. Here, fruits are data, juice maker is the processor and juice is the information that is, received after processing. Information, in its most restricted technical sense, is an ordered sequence of symbols.

1.1.4.3 System:

System ("whole compounded of several parts or members, system", literary "composition") is a set of interacting or interdependent entities forming an integrated whole. The concept of an 'integrated whole' can also be stated in terms of a system embodying a set of relationships which are differentiated from relationships of the set to other elements, and from relationships between an element of the set and elements not a part of the relational regime.

For example, a computer system may be the integration of hardware, software & firmware (i.e. number of hardware parts (say, processor, monitor, keyboard, mouse, etc.), system software, application software as well as program/instructions encoded on semiconductor chips i.e. firmware). Clearly, system software, application software, hardware, etc. are the sub-system which are integrated together to obtain the desired result, known as computer system. Most systems share common characteristics, including: -

Systems have structure, defined by parts and their composition;
Systems have behavior, which involves inputs, processing and outputs of material, energy or information;

Systems have interconnectivity: the various parts of a system have functional as well as structural relationships between each other.

1.1.4.4 Information System: -

An Information System (IS) is any combination of information technology and people's activities using that technology to support operations, management, and decision-making. In a very broad sense, the term information system is frequently used to refer to the interaction between people, algorithmic processes, data and technology. In this sense, the term is used to refer not only to the information and communication technology (ICT) an organization uses, but also to the way in which people interact with this technology in support of business processes.

Some make a clear distinction between information systems, ICT and business processes. Information systems are distinct from information technology in that an information system is typically seen as having an ICT component. Information systems are also different from business processes. Information systems help to control the performance of business processes.

1.1.4.5 Information System Auditing: -

An information systems audit, is an examination of the controls within an information technology infrastructure. An IS audit is the process of collecting and evaluating evidence of an organization's information systems, practices, and operations. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

An IS audit is defined as an audit that encompasses a whole or partial review and evaluation of automated information processing systems, related non-automated
processes and the interfaces between them. This definition provides a very broad
ambit for an IS audit and covers a review of all or any aspect of the information and
communication technology environment from development to deployment, from
planning to monitoring and from acquisition to delivery. IS audit has defined by Ron
Weber as “the process of collecting and evaluating the evidence to determine whether
a computer system (information system) safeguards assets, maintains data integrity,
achieves organizational goals effectively and consumes resources efficiently”.

IS audits are also known as automated data processing (ADP) audits and computer
audits. They were formerly called electronic data processing (EDP) audits.

1.1.4.6 Information System / Technology Controls: -

In business and accounting, information technology controls (or IT controls) are
specific activities performed by persons or systems designed to ensure that business
objectives are met. They are a subset of an enterprise's internal control. IT control
objectives relate to the confidentiality, integrity, and availability of data and the
overall management of the IT function of the business enterprise. IT controls are often
described in two categories: IT general controls ITGC and IT application controls.
ITGC include controls over the information technology (IT) environment, computer
operations, access to programs and data, program development and program changes.
IT application controls refer to transaction processing controls, sometimes called
"input-processing-output" controls. The COBIT Framework (Control Objectives for
Information Technology) is a widely-used framework promulgated by the IT
Governance Institute, which defines a variety of ITGC and application control
objectives and recommended evaluation approaches. IT departments in organizations
are often led by a Chief Information Officer (CIO), who is responsible for ensuring
effective information technology controls are utilized.

1.1.4.6.1 IT/IS General Controls (ITGC): -

ITGC represent the foundation of the IT control structure. They help ensure the
reliability of data generated by IT systems and support the assertion that systems
operate as intended and that output is reliable. ITGC usually include the following
types of controls: -
➤ Control Environment, or those controls designed to shape the corporate culture or "tone at the top."

➤ Change management procedures - controls designed to ensure changes meet business requirements and are authorized.

➤ Source code/document version control procedures - controls designed to protect the integrity of program code

➤ Software development life cycle standards - controls designed to ensure IT projects are effectively managed.

➤ Security policies, standards and processes - controls designed to secure access based on business need.

➤ Incident management policies and procedures - controls designed to address operational processing errors.

➤ Technical support policies and procedures - policies to help users perform more efficiently and report problems.

➤ Hardware/software configuration, installation, testing, management standards, policies and procedures.

➤ Disaster recovery/backup and recovery procedures, to enable continued processing despite adverse conditions.

1.1.4.6.2 IT/IS Application Controls: -

IT application or program controls are fully-automated (i.e., performed automatically by the systems) designed to ensure the complete and accurate processing of data, from input through output. These controls vary based on the business purpose of the specific application. These controls may also help ensure the privacy and security of data transmitted between applications. Categories of IT application controls may include:

Completeness checks - controls that ensure all records were processed from initiation to completion.
Validity checks - controls that ensure only valid data is input or processed.

Identification - controls that ensure all users are uniquely and irrefutably identified.

Authentication - controls that provide an authentication mechanism in the application system.

Authorization - controls that ensure only approved business users have access to the application system.

Input controls - controls that ensure data integrity fed from upstream sources into the application system.

1.2 **Need for Control and Audit of Information Systems:**

The role of information technology (IT) control and audit has become a critical mechanism for ensuring the integrity of information systems (IS) and the reporting of organization finances to avoid and hopefully prevent future financial fiascos such as Enron and WorldCom. Global economies are more interdependent than ever and geopolitical risks impact everyone. Electronic infrastructure and commerce are integrated in business processes around the globe. The need to control and audit never been greater.

Initially, IT auditing (formerly called electronic data processing [EDP], computer information systems [CIC], and IS auditing) evolved as extension of traditional auditing. At that time, the need for an IT audit function came from several directions:

- Auditors realized that computers had impacted their ability to perform the attestation function.

- Corporate and information processing management recognized that computers were key resources for competing in business environment and similar to other valuable business resource within the organization, and therefore, the need for control and audit is critical.
Professional associations and organizations, and government entities recognized the need for IS control and auditability.

The early components of IS auditing were drawn from several areas. First, traditional auditing contributes knowledge of internal control practices and the overall control philosophy. Another contributor was IS management, which provides methodologies necessary to achieve successful design and implementation of systems. The field of behavioural sciences provided such questions and analysis to when and why IS are likely to fail because of people problems. Finally, the field of computer science contributes knowledge about control concepts, discipline, theory, and the formal models that underlie hardware and software design as a basis for maintaining data validity, reliability, and integrity.

IS auditing is an integral part of the audit function because it supports the auditor’s judgment on the quality of the information processed by computer systems. The IS auditor’s role has evolved to provide assurance that adequate and appropriate controls are in place. Of course, the responsibility for ensuring that adequate internal controls are in places rests with the management. The auditor’s primary role, except in areas of management advisory services, is to provide a statement of assurance as to whether adequate and reliable internal controls are in place and are operating in an efficient and effective manner. Therefore, whereas management is to ensure, auditors are to assure.

As we know that computers play vital part in assisting us to process data and to make decisions, it is important that their use be controlled. Therefore, pointed underneath some of the factors that demand for the audit and control: -

1.2.1 **Organizational Costs of Data Loss:**

Data make up a critical resource necessary for an organization's continuing/operations. In this regard, Everest (1985) proposes that data provides the organization with an image of itself, its environment, its history, and its future. If this image is
accurate, the organization increases its abilities to adapt and survive in a changing environment. If this image is inaccurate or lost, the organization can incur substantial losses.

For example, consider a large department store whose accounts receivable file has been destroyed. Unless its customers are honest and also remember what they have purchased from the store, the firm can suffer a major loss in cash receipts through customers failing to pay their debts. The department store's long-run survival could be affected. Consider, also, a department store that loses its accounts payable file. Most likely it will be unable to pay its debts on time. As a result, it could suffer a loss of credit rating as well as any discounts available for early payment. If it contacts creditors requesting their assistance, the department store has to rely on the honesty of its creditors in notifying it of the amounts it owes. Furthermore, creditors might now begin to question the competence of the department store's management. As a result, they might be unwilling to extend credit to the department store in the future.

Such losses can occur when existing controls over computers are lax. For example, management might not provide adequate backup for computer files. Thus, the loss of a file through computer program error sabotage or natural disaster means the file cannot be recovered and the organization's continuing operations are thereby impaired.

1.2.2 Incorrect Decision Making:

Making high-quality decisions depends in part on the quality of the data and the quality of the decision rules that exist within computer-based information system.

The importance of accurate data in a computer system depends on the types of decisions made by persons having some interest in an organization. For example, if managers are making strategic planning decisions, they will probably tolerate some errors in the data, given the long-run nature of strategic planning decisions and the inherent uncertainty surrounding these types of decisions. If managers are making
management control and operational control decisions, however, they will probably require highly accurate data. These types of decisions involve detection, investigation, and correction of out-of-control processes. Thus, in accurate data can cause costly, unnecessary investigations to be undertaken or out-of-control processes to remain undetected. Besides management, incorrect data can also have an impact on other parties who have an interest in an organization.

The importance of having accurate decision rules in a computer system also depends on the types of decisions made by persons having some interest in an organization. In some cases, an incorrect decision rule can have minor consequences. For example, a small, inconsequential error can occur in the calculation of depreciation on a low-value asset. In other cases, however, the consequences can be significant. For example, if the algorithm that determines the interest rate to be paid to customers of a bank is incorrect, the bank might make substantial overpayments to its customers. It might not be able to recover these monies without substantial losses of goodwill. Similarly, if a decision rule in an expert system that supports medical diagnosis is incorrect, doctors could prescribe inappropriate treatments for patients, some of which could be fatal.

1.2.3 Costs of Computer Abuse:

The major stimulus for development of the information systems audit function within organizations often seems to have been computer abuse. Computer abuse is defined to be "any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain." Some major types of computer abuse that an organization might encounter include the following:

| TYPES OF COMPUTER ABUSE |
|-------------------------|-----------------------------|
| Type of Abuse           | Explanation                 |
| Hacking                 | A person gains unauthorized access to a computer system to read, modify or delete programs or data or to disrupt services. |
### Table 1.3

<table>
<thead>
<tr>
<th>Consequences of Abuse</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destruction of assets</td>
<td>Hardware, software, data, facilities, documentation or supplies can be destroyed.</td>
</tr>
<tr>
<td>Theft of assets</td>
<td>Hardware, software, data, documentation or supplies can be illegally removed.</td>
</tr>
<tr>
<td>Modification of assets</td>
<td>Hardware, software, data or documentation can be modified in an unauthorized way.</td>
</tr>
<tr>
<td>Privacy violations</td>
<td>The privacy of data pertaining to a person or an organization can be compromised.</td>
</tr>
<tr>
<td>Disruption of operations</td>
<td>The day-to-day operations of the information systems function can cease temporarily.</td>
</tr>
<tr>
<td>Unauthorized uses of assets</td>
<td>Hardware, software, data, facilities, documentation, or supplies are used for unauthorized purposes (e.g., computer time is used for private consulting purposes).</td>
</tr>
<tr>
<td>Physical harm to personnel</td>
<td>Personnel can suffer physical harm.</td>
</tr>
</tbody>
</table>

### 1.2.4 Value of Computer Hardware, Software and Personnel:

In addition to data, computer hardware, software and personnel are critical organizational resources. Some organizations have multimillion dollar investments in
hardware. Even with adequate insurance, the intentional or unintentional loss of hardware can cause considerable disruption. Similarly, software often constitutes a considerable investment of an organization's resources. If the software is corrupted or destroyed, the organization might be unable to continue operations if it cannot recover the software promptly. If the software is stolen, confidential information could be disclosed to competitors or if the software is a proprietary package, lost revenues or lawsuits could arise. Finally, personnel are always a valuable resource, particularly in light of an ongoing scarcity of well-trained computer professionals in many countries.

1.2.5 High Costs of Computer Error:
Computers now automatically perform many critical functions within our society. For example, they monitor the condition of patients during surgery, direct the flight of a missile, control a nuclear reactor and steer a ship on its course. Consequently, the costs of a computer error in terms of loss of life, deprivation of liberty or damage to the environment can be high. For example, data errors in a computer system used to control flight paths resulted in the death of 257 people when an airplane crashed into a mountain in Antarctica; a person was jailed incorrectly for five months because of erroneous data contained in a computer system.

The costs of computer error in financial terms can also be high. An error in an Australian government computer system resulted in a $126 million overpayment of pharmaceutical benefits. As a result of a human error and deficiencies in its, computer systems design, a company had to pay substantial damages for delivering 93,000 barrels of oil to the wrong consignee. Increasingly, it appears that organizations will be held liable for damages that occur as a result of errors in the design, implementation or operation of their computer systems.

1.2.6 Maintenance of Privacy:
Much data is now collected about us as individuals: taxation, credit, medical, educational, employment, residence and so on. This data was also collected before computers. Nonetheless, the powerful data processing capabilities of computers,
particularly their rapid throughput, integration and retrieval capabilities, cause many people to wonder whether the privacy of individuals (and organizations) has now been eroded beyond acceptable levels. In the United States, for example, civil rights activists have long held substantial concerns about using computer systems for computer-matching purposes (Shattuck 1984). In computer matching, disparate files are merged or compared to build up a profile on a person. A person's taxation data might be compared with data on the social security benefits they receive to detect possible instances of fraud.

More recently, some people have been concerned about the establishment of human genome data banks and the potential to use computers in conjunction with human genetic data to obtain detailed information about a person. They are concerned that knowledge about a person's genetics could be used in decisions about them—for example, whether to give them a job or whether to give them life insurance. Also, some people are concerned about the impact of the Internet on personal privacy. For example, they fear that search engines could be used to extract data from large databases that could compromise a person's privacy.

Aside from any constitutional aspect, many nations deem privacy to be a human right. These nations consider it to be their responsibility of those people concern with computer data processing to ensure that computer use does not evolve to the stage where data about people can be collected, integrated, and retrieved quickly. Furthermore, they consider that computer professionals of all kinds have a responsibility to ensure that data is used only for the purposes intended. Unfortunately, there are now many instances in which computers have been used to abuse the privacy of individuals. As a result, computer professionals are now coming under increasing pressure to ensure that this does not happen.

**Controlled Evolution of Computer Use:**

From time to time, major conflicts arise over how computer technology should be used in our societies. For example, some computer scientists continue to be concerned about using computers to support nuclear weapons command and control systems.
Many became especially vocal during the debate over the U.S. Strategic Defense Initiative's battle management systems. They argue that there liability of complex computer systems usually cannot be guaranteed and that the consequences of using unreliable computer systems can be catastrophic.

Similarly, many people are concerned about the effects that use of computers can have on a person's working life. Should computer technology be allowed to displace people from the workforce or to stultify jobs? What effects do computers have on the physical and mental well-being of their users?

It might be argued that technology is neutral—it is neither good nor bad. The use of technology, however, can produce major social problems. In this light, important, ongoing decisions must be made about how computers should be used in our societies. Governments, professional bodies, pressure groups, organizations and individual persons all must be concerned with evaluating and monitoring how we deploy computer technology.

1.3 **Objective of IS Auditing:**

An IS audit is different from a financial statement audit. While a financial audit's purpose is to evaluate whether an organization is adhering to standard accounting practices, the purposes of an IS audit are to evaluate the system's internal control design and effectiveness. This includes but is not limited to efficiency and security protocols, development processes, and IS governance or oversight. The goal is to evaluate the organization's ability to protect its information assets and properly dispense information to authorized parties. The IS audit's agenda may be summarized by the following questions:

- **Availability:** Will the information systems on which the business is heavily dependent is available for the business at all times when required? Are the systems well protected against all types of losses and disasters?
Confidentiality: Will the information in the systems be disclosed only to those who have a need to see and use it and not any one else?

Integrity: Will the information provided by the systems always be accurate, reliable and timely? What ensures that no unauthorized modification can be made to data or the software in the systems?

Excluding the above mention concerns, others that related with the IS audit are such as effectiveness, efficiency, value for money, return on investment, culture and people related issues. The IS audit focuses on determining risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. By implementing controls, the effect of risks can be minimized, but it cannot completely eliminate all risks.

The information systems auditing supports traditional audit objectives: - attest objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that encompass not only attest objectives but also effectiveness and efficiency objectives. Sometimes information systems auditing has another objective: namely, ensuring that an organization complies with some regulation, rule, or condition. For example, a bank might have to comply with a government regulation about how much it can lend; an introduction agency might seek to comply with a voluntary code in relation to use of personal data about its clients; or an organization might seek to comply with a covenant a loan contract that it has with a merchant bank. Pointed in next page are the four major objectives of information system auditing: -

**Asset Safeguarding Objectives:**

The information system assets of an organization include hardware, software, facilities, people (knowledge), data files, system documentation and supplies. Like all assets, they must be protected by a system of internal control. Hardware can be damaged maliciously. Proprietary software and the contents of data files can be stolen
or destroyed. Supplies of negotiable forms can be used for unauthorized purposes. These assets are often concentrated in one or a small number of locations, such as a single disk. As a result, asset safeguarding becomes an especially important objective for many organizations to achieve.

**Data Integrity Objectives:**

Data integrity is a fundamental concept in information systems auditing. It is a state implying data has certain attributes: completeness, soundness, purity, and veracity. If data integrity is not maintained, an organization no longer has a true representation of itself or of events. Moreover, if the integrity of an organization's data is low, it could suffer from a loss of competitive advantage. Nonetheless, maintaining data integrity can be achieved only at a cost. The benefits obtained should exceed the cost of the control procedures needed.

Three major factors affect the value of a data item to an organization and thus the importance of maintaining the integrity of that data item:

The value of the informational content of the data item for individual decision makers: The informational content of a data item depend on its ability to change the revel of uncertainty surrounding a decision and as a result, to change the expected payoffs of the decisions that might be made. These notions have been wet developed within statistical decision theory.

The extent to which the data item is shared among decision makers: If data is shared, corruption of data integrity affects not just one user but many. The value of a data item is some aggregate function or the value of the data item to the individual users of the data item. Thus, maintenance of data integrity becomes more critical in a shared data environment.
The value of the data item to competitors: If a data item is valuable to a competitor, its loss might undermine an organization's position in the marketplace. Competitors could exploit the informational content of the data item to reduce the profitability of the organization and to bring about bankruptcy, liquidation, takeover or merger.

**System Effectiveness Objectives:**

An effective information system accomplishes its objectives. Evaluating effectiveness implies knowledge of user needs. To evaluate whether a system reports information in a way that facilitates decision making by its users, auditors must know the characteristics of users and the decision-making environment.

Effectiveness auditing often occurs after a system has been running for sometime. Management requests a post audit to determine whether the system is achieving its stated objectives. This evaluation provides input to the decision on whether to scrap the system, continue running it, or modify it in some way.

Effectiveness auditing also can be carried out during the design stages of a system. Users often have difficulty identifying or agreeing on their needs. Moreover, substantial communication problems often occur between system designers and users. If a system is complex and costly to implement, management might want auditors to perform an independent evaluation of whether the design is likely to fulfill user needs.

**System Efficiency Objectives:**

An efficient information system uses minimum resources to achieve its required objectives. Information systems consume various resources: machine time, peripherals, system software and labor. These resources are scarce, and different application systems usually compete for their use. The question of whether an information system is efficient often has no clear-cut answer. The efficiency of any particular system cannot be considered in isolation from other systems. Problems of
sub optimization occur if one system is "optimized" at the expense of other systems. For example, minimizing an application system's execution time might require dedication of some hardware resource (e.g., a printer) to that system. The system might not use the hardware fully, however, while it undertakes its work. The slack resource will not be available to other application systems if it is dedicated to one system.

System efficiency becomes especially important when a computer no longer has excess capacity. The performance of individual application systems degrades (e.g., slower response times occur), and users can become increasingly frustrated. Management must then decide whether efficiency can be improved or extra resources must be purchased. Because extra hardware and software is a cost issue, management needs to know whether available capacity has been exhausted because individual application systems are inefficient or because existing allocations of computer resources are causing bottlenecks. Because auditors are perceived to be independent, management might ask them to assist with or even perform this evaluation.

1.4 Research Design and Methodology:

1.4.1 Objectives of the Study:

The main objectives of the study are pointed underneath:

To determine whether information system auditing and control related to computer system is needed to accomplish the organizational objective especially the banks.

To find out the role efficacy of ICAI (Institute of Chartered Accountants of India) professionals i.e. Chartered Accountants in computer based information system auditing and control of banking sector.

To determine whether it is necessary to pursue information system auditing course through the ICAI Professionals i.e. Chartered Accountants to conduct a computer system audit successfully.
To determine whether there is lack of availability and use of tools and techniques related with computer assisted auditing i.e. generalized audit software, utility software, etc.

To handover a comprehensive understanding regarding the information system audit and control through the review of literature.

1.4.2 Sources of Data and Information: -

The primary data collected through the questionnaires from the Chartered Accountants as well as Managers / Officers of different public bank branches / regional offices. The data through questionnaires are collected from the period of June 2008 to May 2010. The primary data through the questionnaires are collected specifically from Varanasi however for the general observation some of the questionnaires are collected from the different cities of the country such as: - Agra, Allahabad, Anantapur, Chandigarh, East Champaran, Hyderabad, Jaunpur, Lucknow, Mohali, Pratapgarh, and Sonebhadra.

And the secondary data collected from the directory of ICAI members (i.e. Chartered Accountants) as on April 01, 2009 available on the website of the Institute of Chartered Accountants of India (www.icai.org) to study of acquisition status of DISA (Diploma in Information System Audit – a Post Qualification Course on Information System Audit) in India.

Lastly, the other relevant information collected from the books, journals, and websites. References for the same are depicted at the end of the chapters.

1.4.3 Hypotheses: -

Major hypotheses of the study are as follows: -

1. There is significant system for computer based information system auditing and control in banks.
2. There is significant role of ICAI professionals i.e. Chartered Accountants in computer based information system auditing and control of banking sector.

3. There is significant need for the ICAI professionals i.e. Chartered Accountants to pursue the information system auditing course in order to perform the computer based information system audit & control.

1.4.4 Scope and Limitations of the Study: -

The study will handover the details related with overview of information system auditing, framework for information system auditing and key feature of audit software as well as use and functional capabilities of computer assisted auditing techniques through the review of literature and websites. The proposed study will be on the computer based information system audit and control however, study will not cover the other facet of the audit and control. Moreover, the study will deal with the ICAI professionals i.e. Chartered Accountants and not any other professionals for example CISA, etc. Furthermore, the present study also throws light on the status of DISA in Indian States as well as Union Territories of India.

However, study will not provide the details related with the basics of information technology such as computer hardware, software, networking, etc. Further, the proposed study will not discuss any specific audit software in detail related with their functional capabilities as well as study is not going to compare the different audit software.

1.4.5 Methodology: -

The proposed research will be done by composite method including review of literature, web access and survey with questionnaire. The study will involve the visit, communication related with the questionnaire survey from the Banks as well as Chartered Accountants involved in the profession. The primary data collected by the process has tabulated and analyzed as per the drawn hypotheses. The data are segregated between the Varanasi City, Other Cities, & composite of both and number
of response is depicted accordingly. Further, percentage is calculated \(((\text{total YES} / \text{total response}) \times 100)\) and \(((\text{total NO} / \text{total response}) \times 100)\).

Furthermore, the study is based on the secondary data as on April 1, 2009 directory of Chartered Accountants. Each record of Chartered Accountant analyzed for the qualification whether having DISA or not and 148907 members i.e. Chartered Accountants have been checked out of total 153600 members i.e. Chartered Accountants as on April 01, 2009. Approximately 97% of the record have been studied and segregated City wise within the different States / Union Territories of India and only 4693 records i.e. 03.06% are not included in the study due to difficulty in the identification of specific City / State. The complete records are analyzed and segregated on the basis of ACA, FCA and added to calculate the total CA. Moreover the results are tabulated and DISA percentage calculated \(((\text{Total DISA}/\text{Total CA}) \times 100)\) for the different States & Union Territories of India and for the overall India.

1.4.6 Organization of the Study: -

The present study is divided into seven chapters. The first chapter is of introductory nature and discusses the history of information systems auditing, need for control & audit of computer-based information systems; the objectives of information systems auditing; course structure of DISA; and the research design & methodology of the present work. The second chapter throws light on the nature of controls; dealing with complexity; discusses audit risks and procedures; and overview of steps in an audit. Chapter third presents the framework for IS auditing from the system management and control perspective. It deals with the system development life-cycle approach and also evaluates the major phases in system development process. The chapter four focuses on the application control framework. It examines the various application control features which include boundary control, input control, communication control, processing control, database control, and output control. Computer assisted audit techniques has been discussed in fifth chapter with elaboration of audit software such as: - Generalized Audit Software, Industry Specific Audit Software, Utility Software, and Specialized Software. The sixth chapter deals with the data analysis and interpretation. This chapter deals with tabulation, calculation and provided number of charts on the basis of analysis of the data. And in the final seventh chapter findings,
suggestions, and conclusions of the study has been depicted. The complete study is organized in the chapters pointed in next page:

1. Chapter 1 - Overview of Information Systems Auditing
2. Chapter 2 - Conducting an Information Systems Audit
3. Chapter 3 - Management Control Frame Work
4. Chapter 4 - The Application Control Frame Work
5. Chapter 5 - Audit Software (Computer Assisted Audit Techniques)
6. Chapter 6 - Data Analysis and Interpretation
7. Chapter 7 - Findings, Suggestions and Conclusions

References:

8. www.acl.com
10. www.icai.org
11. www.idea.com
12. www.isaca.org