SUPPLEMENT FOR PROFESSIONAL PROGRAMME

NEW SYLLABUS

MODULE 2

INFORMATION TECHNOLOGY AND SYSTEMS AUDIT

Kind attention: The updated study incorporating all the changes covered in this supplement is also available at ICSI website: www.icsi.edu

*Students may also refer the updated study material*
Disclaimer

These Academic Updates have been prepared purely for academic purposes only and it does not necessarily reflect the views of ICSI. Any person wishing to act on the basis of these Academic Updates should do so only after cross checking with the original source. This document is released with an understanding that the Institute shall not be responsible for any errors, omissions and/or discrepancies or actions taken in that behalf.
# CONTENTS

## LESSON 1

**INFORMATION TECHNOLOGY LAW**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Legislative History of Information Technology Act, 2000</td>
<td>2</td>
</tr>
<tr>
<td>Non Applicability of the Act [section 1(4)]</td>
<td>2</td>
</tr>
<tr>
<td>Important Definition under IT Act, 2000</td>
<td>3</td>
</tr>
<tr>
<td>Digital signature</td>
<td>5</td>
</tr>
<tr>
<td>What is a digital signature?</td>
<td>6</td>
</tr>
<tr>
<td>Who issues digital Signature?</td>
<td>6</td>
</tr>
<tr>
<td>Whether digital Signature is permitted/recognised in India?</td>
<td>6</td>
</tr>
<tr>
<td>Provisions relating to Digital Signature and Electronic Signature</td>
<td>6</td>
</tr>
<tr>
<td>Electronic Signature</td>
<td>6</td>
</tr>
<tr>
<td>Electronic records</td>
<td>7</td>
</tr>
<tr>
<td>Authentication of electronic records</td>
<td>7</td>
</tr>
<tr>
<td>Legal Recognition to Electronic Records</td>
<td>7</td>
</tr>
<tr>
<td>Use of Electronic Records</td>
<td>7</td>
</tr>
<tr>
<td>Retention of Electronic Records</td>
<td>7</td>
</tr>
<tr>
<td>Audit of Electronic Records</td>
<td>8</td>
</tr>
<tr>
<td>Validity of Contracts formed through electronic means</td>
<td>8</td>
</tr>
<tr>
<td>Attribution of electronic records</td>
<td>8</td>
</tr>
<tr>
<td>Acknowledgment of receipt of electronic record</td>
<td>8</td>
</tr>
<tr>
<td>Certifying authority</td>
<td>9</td>
</tr>
<tr>
<td>Application for becoming certifying Authority</td>
<td>9</td>
</tr>
<tr>
<td>Renewal of license</td>
<td>9</td>
</tr>
<tr>
<td>Suspension of licence of a Certifying Authority for issuing electronic signature certificates</td>
<td>9</td>
</tr>
<tr>
<td>Certifying Authority to follow certain procedures</td>
<td>10</td>
</tr>
<tr>
<td>Disclosures by Certifying Authority</td>
<td>10</td>
</tr>
<tr>
<td>Controller of Certifying Authority</td>
<td>10</td>
</tr>
<tr>
<td>Functions of the Controller</td>
<td>10</td>
</tr>
</tbody>
</table>
Recognition of foreign Certifying Authorities

Electronic signature certificates

Representations upon issuance of Digital Signature Certificate

Suspension of Digital Signature Certificate

Revocation of Digital Signature Certificate

Notice of suspension or revocation

Cyber appellate tribunal (CAT)

Constitution of Cyber Appellate Tribunal

Bench of Cyber Appellate Tribunal

Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal

Term of office, conditions of service etc of Chairperson and Members

Resignation and removal

Powers of the Chairman of Cyber Appellate Tribunal

Appeal to Cyber Appellate Tribunal

Procedure and Powers of the Cyber Appellate Tribunal

Appeal to High Court

Compounding of Contravention

Offences and Penalties under Information Technology Act, 2000

Computer related offence

Compensation for failure to protect data (Section 43A)

Penalty for failure to furnish information, return, etc.

Residuary Penalty

Tampering with computer source documents

Punishment for sending message through communication service etc.

Punishment for dishonestly receiving or retaining any stolen computer resource or communication device

Punishment for Identity theft

Punishment for cheating by personation by using computer resource

Punishment for Violation of privacy

Punishment for Cyber terrorism

Punishment for Publishing or transmitting of material obscene material in electronic form

Punishment for Publishing or transmitting of material containing sexually explicit act, etc. in electronic form

Punishment for Publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form
Publishing of information which is obscene in electronic form [section 67] 19
Penalty for Misrepresentation [section 71] 19
Penalty for breach of confidentiality [section 72] 19
Punishment for disclosure of information in breach of lawful contract 19
Penalty for publishing false electronic signature Certificate [section 73] 20
Penalty for fraudulent publication [section 74] 20
LESSON ROUND-UP 20
SELF-TEST QUESTIONS 21

LESSON 11
SYSTEMS AUDIT – AN OVERVIEW

Introduction 24
Definition of System Audit 24
Objectives of Information system audit 25
Nature, significance and scope of systems audit 26
Nature of System Audit 26
Significance of System Audit 26
Scope of Information System Audit 27
Steps involved in conducting systems audit 28
Systems audit & management functions 29
System audit of different functions 30
Audit of management controls 31
Security Policy and Standards 31
Steering Committee for Security 31
Business Continuity Planning 31
Systems Development Methodology 31
Audit of operational controls 32
Audit of Environmental Controls 32
Audit of organizational controls 33
Systems audit of computerized secretarial functions 34
Application controls 34
Norms and procedures for computerization 35
What Should Be Automated? 35
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasons for Automation</td>
<td>36</td>
</tr>
<tr>
<td>Automation should facilitate daily operations and planning.</td>
<td>36</td>
</tr>
<tr>
<td>Procedure of computerisation</td>
<td>37</td>
</tr>
<tr>
<td>Assessment and Planning</td>
<td>37</td>
</tr>
<tr>
<td>Conducting an Initial Assessment</td>
<td>38</td>
</tr>
<tr>
<td>Developing Goals, Objectives and Priorities</td>
<td>39</td>
</tr>
<tr>
<td>Purpose of the System</td>
<td>39</td>
</tr>
<tr>
<td>Technical Considerations</td>
<td>39</td>
</tr>
<tr>
<td>Organisational Factors</td>
<td>40</td>
</tr>
<tr>
<td>Resource Requirements</td>
<td>40</td>
</tr>
<tr>
<td>Political Issues</td>
<td>40</td>
</tr>
<tr>
<td>Computers Control and Security</td>
<td>41</td>
</tr>
<tr>
<td>Testing of computer systems – Documentation standards, policies and procedures and audit approach</td>
<td>43</td>
</tr>
<tr>
<td>Documentation of the system</td>
<td>43</td>
</tr>
<tr>
<td>Narrative Descriptions</td>
<td>43</td>
</tr>
<tr>
<td>Flowcharts</td>
<td>44</td>
</tr>
<tr>
<td>Organisation Charts</td>
<td>45</td>
</tr>
<tr>
<td>Minimum Contents of System Documentation</td>
<td>45</td>
</tr>
<tr>
<td>Annexure A</td>
<td>46</td>
</tr>
<tr>
<td>LESSON ROUND-UP</td>
<td>49</td>
</tr>
<tr>
<td>SELF-TEST QUESTIONS</td>
<td>50</td>
</tr>
</tbody>
</table>
Lesson 1
Information Technology Law

LESSON OUTLINE

– Information Technology Act – Definitions.
– Important terms under Information Technology Legislation.
– Digital Signatures
– Electronic Records
– Certifying Authority
– Electronic Signature Certificate
– Cyber Appellate Tribunal
– Offences and Penalties

LEARNING OBJECTIVES

In present scenario, Computer and Internet has impacted most of us. Information technology has proved to be boon for humanity and it has benefited the human life in many ways. Since with every positive thing, some negatives also creep in, similarly people also started to misuse the wonders of information technology. In year 2000, information technology Act, 2000 was passed to deal with various matters pertaining to Information Technology, its uses and misuses. Information technology Act, 2000 provides legal recognition to electronic communication, email, digital signatures, computerized documents and it also provides for legal remedies in case of misuse of information technology. After reading this lesson, a student will be able to understand –

– The meaning of different terms as used in Information technology Act, 2000
– The meaning of digital signatures, electronic records
– The working of certifying authority appointed for issuing digital signatures
– The working of cyber regulation Appellate tribunal
– The consequences of various offences made under the Acts and penalty for such offences

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternative to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the India Evidence Act, 1872, the Banker’s Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
INTRODUCTION


The Information Technology Act, 2000 was made applicable in India with following objectives

1. To give legal recognition to any transaction which is done electronically or use of internet?
2. To give legal recognition to digital signature for accepting any agreement via computer.
3. To provide facility of filling document online relating to school admission or registration in employment exchange.
4. To provide legal recognition for storage in electronic format.
5. To stop computer crime and protect privacy of internet users.
6. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
7. To amend the Indian Penal Code, Indian Evidence Act, 1872, The Bankers’ Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934

Legislative History of Information Technology Act, 2000

Information Technology Act, 2000 was primarily based on UNICITRAL model law on e-commerce. Attempts were made in year 1998 for introducing law pertaining to Information Technology in India but the Information Technology Act, 2000 was passed only in June, 2000. The Government of India has brought major amendments to Information Technology Act, 2000 in form of the Information Technology Amendment Act, 2008. Information Technology Amendment Act 2008 is the new version of Information Technology Act, 2000 and it has provided additional focus on Information Security. It has added several new sections on offences including Cyber Terrorism and Data Protection

Territorial Jurisdiction of the Act: Information Technology Act, 2000 extends to the whole of India including the state of Jammu and Kashmir. Unless otherwise provided in this Act, Information Technology Act, 2000 also applies to any offence or contravention hereunder committed outside India by any person.

Non Applicability of the Act [section 1(4)]

Information Technology Act, 2000 is not be applicable to –

(a) A negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
(b) A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
(c) A trust as defined in section 3 of the Indian Trusts Act, 1882;
(d) A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
(e) Any contract for the sale or conveyance of immovable property or any interest in such property;
(f) Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.
Important Definition under IT Act, 2000

2(1) (a) “Access” with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

2(1) (b) “Addressee” means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

2(1) (c) “Adjudicating officer” means an adjudicating officer appointed under subsection (1) of section 46;

2(1) (d) “Affixing digital signature” with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

2(1) (e) “Appropriate Government” means as respects any matter,—
   (i) Enumerated in List II of the Seventh Schedule to the Constitution;
   (ii) Relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

2(1) (f) “Asymmetric crypto system” means a system of a secure key pair consisting of a Private Key for creating a digital signature and a public key to verify the digital signature;

2(1) (g) “Certifying Authority” means a person who has been granted a license to issue a Digital Signature Certificate under section 24;

2(1) (h) “Certification practice statement” means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

2(1) (i) “Computer” means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

2(1) (j) “Computer network” means the interconnection of one or more computers through—
   (i) The use of satellite, microwave, terrestrial line or other communication media; and
   (ii) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

2(1) (l) “Computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

2(1) (m) “Controller” means the Controller of Certifying Authorities appointed under sub-section (l) of section 17;

2(1) (n) “Cyber Appellate Tribunal” means the Cyber Regulations Appellate Tribunal established under subsection (1) of section 48;

2(1) (o) “Data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
2(1) (p) “Digital signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

2(1) (q) “Digital Signature Certificate” means a Digital Signature Certificate issued under subsection (4) of section 35;

2(1) (r) “Electronic form” with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

2(1) (s) “Electronic Gazette” means the Official Gazette published in the electronic form;

2(1) (t) “Electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

2(1) (v) “Information” includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:

2(1) (w) “Intermediary” with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

2(1) (x) “Key pair”, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

2(1) (za) “Originator” means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

2(1) (zc) “Private Key” means the key of a key pair used to create a digital signature;

2(1) (zd) “Public key” means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

2(1) (ze) “Secure system” means computer hardware, software, and procedure that—

(a) Are reasonably secure from unauthorized access and misuse;

(b) Provide a reasonable level of reliability and correct operation;

(c) Are reasonably suited to performing the intended functions; and

(d) Adhere to generally accepted security procedures;

2(1) (zh) “Verify” in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) The initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

Further, explanation to Section 43 and Section 43A of the Information Technology Act, 2000 defines the following terms

(i) “Computer contaminant” means any set of computer instructions that are designed –

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;
(ii) “computer data base” means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) “computer virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) “damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means

(v) “Computer Source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form (Inserted vide ITAA 2008)

(vi) “Body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(vii) “Reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(viii) “Sensitive personal data or information” means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Explanation to Section 66 E of the Information Technology Act, 2000 defines the following terms.

(a) “Transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “Capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “Private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast:

(d) “Publishes” means reproduction in the printed or electronic form and making it available for public;

(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that –

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public regardless of whether that person is in a public or private place.

**DIGITAL SIGNATURE**

As per Section 2(1) (p) of Information Technology Act, 2000 “Digital signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

Before going into details about provisions relating to digital signature, here it is important to understand the basic concepts relating to digital signature
What is a digital signature?

A Digital signature (standard electronic signature) takes the concept of traditional paper-based signing and turns it into an electronic “fingerprint.” This “fingerprint,” or coded message, is unique to both the document and the signer and binds both of them together. The digital signature ensures the authenticity of the signer. Any changes made to the document after it is signed invalidate the signature, thereby protecting against signature forgery and information tampering. Digital signatures help organizations to sustain signer authenticity, accountability, data integrity and non-repudiation of electronic documents and forms.

Who issues digital Signature?

A digital signature is issued by a Certification Authority (CA) and is signed with the CA's private key. A digital signature/electronic signature typically contains the: Owner’s public key, the Owner’s name, Expiration date of the public key, the Name of the issuer (the CA that issued the Digital ID), Serial number of the digital signature, and the digital signature of the issuer. Digital signatures deploy the Public Key Infrastructure (PKI) technology.

Whether digital Signature is permitted/recognised in India?

In India, recognition to digital signature has been given by Income Tax Act, 1961 and Companies Act, 2013. As per provisions of Companies Act, 2013, directors of the companies are required to sign their document by means of digital signature only. Similarly If one file his Income Tax return electronically using digital signature he does not have to submit a physical copy of the return. While in case of paper based signature, one need to physically submit the printed copy of the filled up Form along with the copy of the Provisional Acknowledgement Number of e-Return.

Provisions relating to Digital Signature and Electronic Signature

As per section 3 of Information Technology Act, 2000 as amended, any subscriber may authenticate an electronic record by affixing his digital signatures. The authentication of the electronic records shall be effected by the use of asymmetric crypto system and hash function which envelops and transform the electronic records into another electronic record.

Explanation to Section 3 of the Information Technology Act, 2000 defines hash function. As per the explanation provided, hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known' as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) To derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) That two electronic records can produce the same hash result using the algorithm.

Any person by the use of a public key of the subscriber can verify the electronic record. Here, the private key and the public key are unique to the subscriber and constitute a functioning key pair.

Electronic Signature

The provisions relating to electronic signature have been added by IT Information Technology (Amendment) Act, 2008. Section 3A of Information Technology Act, 2000 provides for authentication of electronic record by such electronic signature or electronic authentication technique which is considered reliable.

Any electronic signature or electronic authentication technique shall be considered reliable if—

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
(c) any alteration to the electronic signature made after affixing such signature is detectable;
(d) any alteration to the information made after its authentication by electronic signature is detectable; and
(e) it fulfils such other conditions which may be prescribed.

The government has yet not notified the electronic signature or electronic authentication technique.

**ELECTRONIC RECORDS**

As per Section 2(t) of Information Technology Act, 2000, “Electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

**Authentication of electronic records**

As per Section 3 of Information Technology Act, 2000, any subscriber may authenticate an electronic record by affixing his digital signature. The authentication of the electronic record are effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. ‘Hash function’ means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result”. An electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) that two electronic records can produce the same hash result using the algorithm.

The private key and the public key are unique to the subscriber and constitute a functioning key pair. The electronic records can be verified by a person by the use of a public key of the subscriber.

**Legal Recognition to Electronic Records**

Section 4 of Information Technology Act, 2000 provides legal recognition to Electronic Records. As per Section 4 of the Act, where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference.

**Use of Electronic Records**

As per Section 6 of Information Technology Act, 2000, where any law provides for the filing of any form application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner; and the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner; and the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

**Retention of Electronic Records**

Section 7 of the Information Technology Act, 2000 provides for retention of records in electronic format. Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, provided—

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;
(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. These provisions will not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Audit of Electronic Records
As per Section 7A of Information Technology Act, 2000 where in any law, there is a provision of audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information maintained in the electronic form.

Validity of Contracts formed through electronic means
Section 10A of the Information Technology Act, 2000 provides that where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means are used for that purpose.

Attribution of electronic records.
Section 11 of Information Technology Act, 2000 provides that an electronic record shall be attributed to the originator if it was sent by the originator himself; or by a person who had the authority to act on behalf of the originator in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically.

Acknowledgment of receipt of electronic record
Section 12 of Information Technology Act, 2000 provides where the originator has not agreed that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Time and place of despatch and receipt of electronic record
Section 13 of the Information Technology Act, 2000 contains the provisions relating to ascertainment of time and
place of dispatch and receipt of electronic records. Unless agreed otherwise between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

If the addressee has designated a computer resource for the purpose of receiving electronic records, receipt occurs at the time when the electronic record enters the designated computer resource; or if the electronic record is sent to a non-designated computer resource of the addressee, receipt occurs at the time when the electronic record is retrieved by the addressee.

If the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

Unless agreed otherwise, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business. If the originator or the addressee has more than one place of business, the principal place of business shall be the place of business. If the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business.

**CERTIFYING AUTHORITY**

A Certifying Authority is a trusted body whose central responsibility is to issue, revoke, renew and provide directories of electronic Certificates. According to section 2(g) of Information Technology Act, 2000 “Certifying Authority” means a person who has been granted a license to issue Electronic Signature Certificates.

**Application for becoming certifying Authority**

Any person may make an application, to the Controller of certifying authorities, for a license to issue Electronic Signature Certificates provided he fulfills the Central Government prescribed requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue electronic Signature Certificates.

A license granted for issuing Electronic Signature Certificate is valid for 5 years and it is not transferable or heritable. The license is subject to the terms and conditions as prescribed by Information Technology (Certifying Authorities) Rules, 2000.

Every application for issue of a license shall be in made in form as prescribed by Schedule-I of Information Technology (Certifying Authorities) Rules, 2000 and the application shall be accompanied by a certification practice statement; A statement including the procedures with respect to identification of the applicant; Payment of fees of twenty-five thousand rupees and other documents, as prescribed by Information Technology (Certifying Authorities) Rules, 2000.

**Renewal of license**

A certifying Authority can apply for renewal of license not less than forty-five days before the date of expiry of the period of validity of licence and comply all the rules of Information Technology (Certifying Authorities) Rules, 2000 which are applied in case of fresh application for becoming certifying Authority.

The Controller may, on receipt of an application for appointment as certifying authority, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application: No application for becoming certifying Authority shall be rejected under unless the applicant has been given a reasonable opportunity of presenting his case.

**Suspension of licence of a Certifying Authority for issuing electronic signature certificates**

The Controller of Certifying Authority may revoke the license of certifying authority, if after proper enquiry, he is
satisfied that a certifying authority has made a false or incorrect statement in material particulars in, or in relation to, the application for the issue or renewal of the licence and/or it has failed to comply with the terms and conditions subject to which the licence was granted and/or it has failed to maintain the standards as specified and/or contravened any provisions of the Act, rule, regulation or order made there under. However no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

The Controller of certifying authority may, if he has reasonable cause to believe that there is any ground for revoking a licence, by order suspend such licence pending the completion of any inquiry ordered by him provided no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension. The Certifying Authority whose licence has been suspended will not issue any Digital Signature Certificate during such suspension.

Certifying Authority to follow certain procedures

Every Certifying Authority shall make use of hardware, software and procedures that are secure from intrusion and misuse and it will provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions. It will adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and observe such other standards as may be specified by regulations.

Disclosures by Certifying Authority

Every Certifying Authority shall disclose in the manner specified by regulations—(a) its Electronic Signature (b) any certification practice statement relevant thereto; (c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and (d) any other fact that materially and adversely affects either the reliability of a Electronic Signature Certificate, which that Authority has issued, or the Authority’s ability to perform its services.

Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Electronic Signature Certificate was granted, then, the Certifying Authority shall use reasonable efforts to notify any person who is likely to be affected by that occurrence; or act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Controller of Certifying Authority

As per Section 17 of IT Act, 2000 as amended, The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities and such number of Deputy Controllers and Assistant Controllers as it deems fit for the purpose of this Act.

The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government and The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

Functions of the Controller

The Controller may perform all or any of the following functions, namely:—

(a) Exercising supervision over the activities of the Certifying Authorities;
(b) Certifying public keys of the Certifying Authorities;
(c) Laying down the standards to be maintained by the Certifying Authorities;
(d) Specifying the qualifications and experience which employees of the Certifying Authorities should possess;
(e) Specifying the conditions subject to which the Certifying Authorities shall conduct their business;
(f) Specifying the contents of written, printed or visual materials and Advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) Specifying the form and content of a Digital Signature Certificate and the Key,

(h) Specifying the form and manner in which accounts shall be maintained by The Certifying Authorities;

(i) Specifying the terms and conditions subject to which auditors may be Appointed and the remuneration to be paid to them;

(j) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) Specifying the manner in which the Certifying Authorities shall conduct their Dealings with the subscribers;

(l) Resolving any conflict of interests between the Certifying Authorities and the Subscribers;

(m) Laying down the duties of the Certifying Authorities;

(n) Maintaining a data base containing the disclosure record of every Certifying

(o) Authority containing such particulars as may be specified by regulations, which shall Be accessible to public.

Recognition of foreign Certifying Authorities

The Controller of Certifying Authority may recognize the foreign certifying authority with the prior approval of the Central Government provided the foreign certifying authority fulfill the prescribed conditions and restrictions. Where any foreign Certifying Authority is recognised, the electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act. The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition , he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

ELECTRONIC SIGNATURE CERTIFICATES

The provisions relating to Electronic Signature Certificate are contained in Section 35-39 of Information Technology Act, 2000. It provides that Certifying Authority will issue Electronic Signature Certificate on an application by a person in the form prescribed by the Central government. The application should be accompanied by a fee not exceeding Rs. 25,000/- and a certificate practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

On receipt of an application, the Certifying Authority may, after consideration of the certification practice statement or the other prescribed statement and after making such enquiries as it may deem fit, grant the electronic Signature Certificate or for reasons to be recorded in writing, reject the application, however no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Representations upon issuance of Digital Signature Certificate

Section 36 of Information Technology Act, 2000 provides that –

A Certifying Authority while issuing a Digital Signature Certificate shall certify that –

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder,

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature
Certificate;

(ca) The subscriber holds a private key which is capable of creating a digital signature:

(cb) The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;

(d) the subscriber’s public key and private key constitute a functioning key pair,

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

Suspension of Digital Signature Certificate

The provisions relating to Suspension of Digital Signature Certificate are contained in Section 37 of IT Act, 2000 as amended. This provides that the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate, —

(a) on receipt of a request to that effect from—
   (i) the subscriber listed in to Digital Signature Certificate; or
   (ii) any person duly authorized to act on behalf of that subscriber,

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Revocation of Digital Signature Certificate

The provisions relating to Suspension of Digital Signature Certificate are contained in Section 38 of Information Technology Act, 2000

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it –

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber, or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that —

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority’s private key or security system was compromised in a manner materially affecting the Digital Signature Certificate’s reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.
(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

**Notice of suspension or revocation**

The provisions relating to Suspension of Digital Signature Certificate are contained in Section 39 of IT Act, 2000 as amended.

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

**CYBER APPELLATE TRIBUNAL (CAT)**

Cyber Appellate Tribunal has been established by the Central Government in accordance with the provisions under Section 48(1) of the Information Technology Act, 2000 under the aegis of Controller of Certifying Authorities (C.C.A.).

**Constitution of Cyber Appellate Tribunal**

The composition of the Cyber Appellate Tribunal is provided for under section 49 of the Information Technology Act, 2000. Initially the Tribunal consisted of only one person who was referred to as the Presiding Officer but in year 2008, the composition of Cyber Appellate Tribunal was changed.

As per the amended section the Tribunal shall consist of a Chairperson and such number of other Members as the Central Government may by notification in the Official Gazette appoint. The selection of the Chairperson and Members of the Tribunal is made by the Central Government in consultation with the Chief Justice of India. The Presiding Officer of the Tribunal is now known as the Chairperson.

**Bench of Cyber Appellate Tribunal**

The Chairperson of the Cyber Appellate Tribunal may constitute a Bench of the tribunal consisting with one or two members of such Tribunal as the Chairperson may deem fit. Every bench of the tribunal shall be presided over by the Chairperson or the Judicial Member appointed under sub-section (3) of section 50 of the Information Technology Act, 2000. The bench of the tribunal may exercise the jurisdiction, powers and authority of the Cyber Appellate Tribunal. The Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify. The central government will notify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction. The chairman of the appellate tribunal has been given the power of transferring a member of tribunal from bench to another bench of the tribunal. If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.

**Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal**

Section 50 of the Information Technology Act, 2000 provides the qualification for appointing a person as the chairperson or members of the Central Appellate Tribunal

A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is,
or has been, or is qualified to be, a Judge of a High Court. The Members of the Cyber Appellate Tribunal, except
the Judicial Member hall be appointed by the Central Government from amongst persons, having special
knowledge of, and professional experience in, information technology, telecommunication, industry, management
or consumer affairs Provided such person is in the service of the Central Government or a States Government,
and has held the post of Additional Secretary to the Government of India or any equivalent post in the Central
Government or State Government for a period of not less than one year or Joint Secretary to the Government of
India or any equivalent post in the Central Government or State Government for a period of not less than seven
years.

The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from
amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional
Secretary for a period of not less than one year or Grade I post of that Service for a period of not less than five
years.

**Term of office, conditions of service etc of Chairperson and Members**

The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the
date on which he enters upon his office or until he attains the age of sixty five years, whichever is earlier. Before
appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government
shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially
his functions as such Chairperson or Member. An officer of the Central Government or State Government on his
selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire
from service before joining as such Chairperson or Member.

**Resignation and removal**

(1) The Presiding officer Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under
his hand addressed to the Central Government, resign his office Provided that the said Presiding officer
Chairperson or Member shall, unless he is permitted by the Central Government to relinquish his office sooner,
continue to hold office until the expiry of three months from the date of receipt of such notice or until a person
duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the
earliest.

(2) The Presiding officer Chairperson or Member of a Cyber Appellate Tribunal shall not be removed from his
office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after
an inquiry made by a Judge of the Supreme Court in which the Chairperson or Member concerned has been
informed of the charges against him and given a reasonable opportunity of being heard in respect of these
charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or
incapacity of the aforesaid Presiding officer Chairperson or Member.

**Powers of the Chairman of Cyber Appellate Tribunal**

The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions
in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the
Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed. Where
Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business
of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench. On the application of
any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be
heard, or suo motu without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case
pending before one Bench, for disposal to any other Bench.
Appeal to Cyber Appellate Tribunal

Any person aggrieved by an order made by a Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. If an order is made by the adjudicating officer with the consent of the parties, No appeal shall lie to the Cyber Appellate Tribunal. Every appeal shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed. However the Cyber Appellate Tribunal may entertain an appeal even after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period. On receipt of an appeal, the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against. The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer. The appeal filed before the Cyber Appellate Tribunal shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

Procedure and Powers of the Cyber Appellate Tribunal

The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

For the purposes of discharging their functions under this Act, The Cyber Appellate Tribunal shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -

(a) summoning and enforcing the attendance of any person and examining him on oath;
(b) requiring the discovery and production of documents or other electronic records;
(c) receiving evidence on affidavits;
(d) issuing commissions for the examination of witnesses or documents;
(e) reviewing its decisions;
(f) dismissing an application for default or deciding it ex parte
(g) any other matter which may be prescribed

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

Appeal to High Court

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order however the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period of 60 days may allow it to be filed within a further period not exceeding sixty days.

Compounding of Contravention

Section 63 of the Information Technology Act, 2000 provides for the compounding of contravention under this Act. Any contravention under this Act may, either before or after the institution of adjudication proceedings, be
compounded by the Controller or an officer person authorized by him, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify: Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded. No compounding of contravention may be done to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded. Where any contravention has been compounded, no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

OFFENCES AND PENALTIES UNDER INFORMATION TECHNOLOGY ACT, 2000

Computer related offence

Section 65 to Section 67 of the Information Technology Act, 2000 deals with computer related offences. Computer related offences have been defined in section 43 of the Information Technology Act, 2000 which provides that if any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network,-

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there-under;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or any other computer source code used for a computer resource with an intention to cause damage;

She/he would be liable to pay compensation to the party so affected and shall be punishable with imprisonment for a term which may extend to life imprisonment or with fine which may extend to one crore or both.

Compensation for failure to protect data (Section 43A)

As per section 43A of Information Technology Act, 2000 where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation...
to the person so affected.

**Penalty for failure to furnish information, return, etc.**

As per section 44 of Information Technology Act, 2000 as amended, If any person who is required under this Act or any rules or regulations made there under to -

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:

(c) Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

**Residuary Penalty**

Section 45 of Information Technology Act, 2000 provides whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

**Tampering with computer source documents**

Section 65 of the Information Technology Act, 2000 provides for punishment upto three years or with a fine which may extend upto Rs. 2 lakhs or with both whoever knowingly or intentionally tampers with the computer code source documents.

**Punishment for sending message through communication service etc.**

Section 66A of the Information Technology Act, 2000 has been strike down by the Hon’ble Supreme Court of India vide its decision dated 24th March, 2015.

**Punishment for dishonestly receiving or retaining any stolen computer resource or communication device**

As per section 66B of the Information Technology Act, 2000, whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

**Punishment for Identity theft**

As per section 66C of the Information Technology Act, 2000, Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

**Punishment for cheating by personation by using computer resource**

As per section 66D of the Information Technology Act, 2000, whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a
term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee.

### Punishment for Violation of privacy

As per section 66E of the Information Technology Act, 2000 whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

### Punishment for Cyber terrorism

As per 66F of the Information Technology Act, 2000 whoever,—(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

1. denying or cause the denial of access to any person authorized to access computer resource; or
2. attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
3. introducing or causing to introduce any computer contaminant;

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.'.

### Punishment for Publishing or transmitting of material obscene material in electronic form

As per 67 of the Information Technology Act, 2000 whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

### Punishment for Publishing or transmitting of material containing sexually explicit act, etc. in electronic form

As per 67A of the IT Act, whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
### Punishment for Publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

As per 67B of the IT Act, whoever, –

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form—

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes.

### Publishing of information which is obscene in electronic form [section 67]

Section 67 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to 5 years and with fine which may extend to Rs. 1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to ten years and fine which may extend to Rs. 2 lakhs.

### Penalty for Misrepresentation [section 71]

This section provides that any person found misrepresenting or suppressing any material fact from the Controller or the Certifying Authority shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

### Penalty for breach of confidentiality [section 72]

Section 72 provides a punishment for breach of confidentiality and privacy of electronic records, books, information etc. by a person who has access to them without the consent of the person to whom they belong with imprisonment for a term which may extend to 2 years or with a fine which may extend to Rs. 1 lakh or with both.

### Punishment for disclosure of information in breach of lawful contract

Section 72A of the Act provides. Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or
in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years or with a fine which may extend to five lakh rupees or with both.

**Penalty for publishing false electronic signature Certificate [section 73]**

This section provides punishment for publishing a **electronic signature Certificate** false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

**Penalty for fraudulent publication [section 74]**

This section provides for punishment with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both to a person whoever knowingly publishes for fraudulent purpose any **electronic Signature Certificate**.

**LESSON ROUND-UP**

- The Information Technology Act, 2000 was come into effect in year 2000 and it was further amended in Year 2008 by IT Amendment Act, 2008.

- This Act aims to provide the legal infrastructure for e-commerce in India. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers’ Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

- Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

- Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference. The said chapter also details the legal recognition of Electronic Signatures.

- Chapter-VI of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Electronic Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Electronic Signature Certificates.

- Chapter-VII of the Act details about the scheme of things relating to Electronic Signature Certificates. The duties of subscribers are also enshrined in the said Act.

- Chapter-IX of the said Act talks about penalties, Compensation and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating
Officer for holding an inquiry in the manner prescribed by the Central Government. The adjudicating officer shall exercise jurisdiction to adjudicate matters in which the claim for inquiry or damage does not exceed Five Crore rupees.

– Chapter-X of the Act talks of the establishment of the Cyber Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

– Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Inspector of Police. These offences include tampering with computer source documents, Computer related offences, publishing of information, which is obscene in electronic form, cyber terrorism etc.

**SELF-TEST QUESTIONS**

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. Explain briefly the scope of the Information Technology Act 2000 as amended along with the relevant definitions that are used.

2. What are the conditions subject to which electronic record may be authenticated by means of affixing electronic signature?

3. Discuss the main provisions provided in Information Technology Act 2000 as amended to facilitate E-governance

4. What are the regulations relating to the appointment and powers of the certifying authorities under Chapter VI, Section 17 to 25 of Information Technology Act 2000 as amended?

5. What are the duties of a certifying authority under Section 30 of the Information Technology Act 2000 as amended?

6. What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage?

7. Write short notes on the following:
   (a) Electronic Signature Certificate
   (b) Encryption.

8. Describe the composition and powers of Cyber appellate tribunal.


10. Briefly explain the power of central government to make rules with respect to the Section 10 of Information Technology Act 2000 as amended.

11. Explain the power of Controller to make regulations under Section 89 of the Information Technology Act 2000 as amended.

12. What are the powers of a Police Officer under the Information Technology (Amendment) Act 2008 to enter and search etc?


14. Briefly explain the Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form as per Section 67 A of The Information Technology Act ,2000 as amended
Lesson 11
Systems Audit – An Overview

LESSON OUTLINE

- Nature, Significance and Scope of Systems Audit
- Steps Involved in Conducting Systems Audit
- Systems Audit and Management Functions
- Systems Audit of Computerized Secretarial Functions
- Norms and Procedure for Computerization, Computers Control and Security

LEARNING OBJECTIVES

Information systems auditing or systems audit is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently. Information system audit is done to verify that systems and its various applications are appropriate, efficient and adequately controlled. Information system audit is carried out to ensure valid, reliable, timely and secure input processing and output at all levels of a system’s activity. System audit supports traditional audit objectives and also helps management in achieving various control objectives.

Technology plays a major role in facilitating all functions of business in this era, not just in transaction capturing and processing but even in lesser known areas like Corporate Governance and Risk Management. With changing paradigms, knowledge and experience in technology are not merely desirable, but basic requirements for growth and even survival in the evolving global village. Information system audit also seeks to leverage technology to enhance the professional skills of its users. In view of above, it become necessary for a company secretary to know about basic concepts relating to systems audit. After going through this lesson, one should be able to –

- Understand about the nature and scope of system audit
- Understand the information system audit process
- Understand the relationship between information system audit and different functions of management.
- Design a information system audit plan
  Carry out the system audit of secretarial function

The systems audit, unlike the other audits, is not restricted to audit of reported items only. It has to take into cognizance the choice, use and risk of Technology. It has to look at the realities of business processes and constantly changing legal framework.
INTRODUCTION

As computer technology has advanced, most of the organisations have become increasingly dependent on computerised information systems to carry out their operations and to process, maintain, and report essential information. As a consequence, the reliability of computerised data and of the systems that process, maintain and report these data are a major concern to audit. Information system auditor mainly known as IT Auditors evaluate the reliability of computer generated data supporting financial statements and analyse specific programs and their outcomes. In addition, IT Auditors examine the adequacy of controls in information systems and related operations to ensure system effectiveness.

IT Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organisational goals to be achieved effectively, and uses resources efficiently. Data integrity relates to the accuracy and completeness of information as well as to its validity in accordance with the norms. An effective information system leads the organisation to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives. IT Auditor must know the characteristics of users of the information system and the decision making environment in the auditee organisation while evaluating the effectiveness of any system.

Use of computer facilities has brought about radically different ways of processing, recording and controlling information and has combined many previously separated functions. The potential for material systems error has thereby been greatly increased causing great costs to the Organisation, e.g., the highly repetitive nature of many computer applications means that small errors may lead to large losses. An error in the calculation of Income Tax to be paid by employees in a manual system will not occur in each case but once an error is introduced in a computerised system, it will affect each case. A bank may suffer huge losses on account of an error of rounding off to next rupee instead of nearest rupee. This makes it imperative for the auditor to test the invisible processes, and to identify the vulnerabilities in a computer information system as the costs involved, because of errors and irregularities, can be high. Company Secretary Professional is not different from this. Company Secretary cannot function effectively in this information age without adequate knowledge of information system, its benefits and limitations. The Company Secretary addresses the vital areas of good corporate governance and compliance within the regulatory framework of the applicable laws. Besides handling secretarial functions, s/he is also a custodian and user of the top level MIS that goes to the Board of Directors.

This study lesson has been prepared to provide an insight into the subject of systems audit in the modern context of enterprise systems and connectivity with buyers, suppliers and other stakeholders.

DEFINITION OF SYSTEM AUDIT

The legendary Ron Weber defines IT Audit as “the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organisational goals to be achieved effectively and uses resources efficiently”.

IT Audit is a broad term that includes Financial Audits (to assess the correctness of an organization’s financial statements), Operational Audits (evaluation of internal control structure), Information Systems Audit( including performance Audit), Specialized Audits (evaluation of services provided by a third party such as outsourcing etc.) and Forensic Audits. However, a common factor is the formation of an opinion regarding the degree of reliance that can be placed on the IT systems in the audited organization. Audits of Information Technology Systems under development and IT enabled audits (using CAATs) also fall under this broad Grouping.

Information systems’ audit represents a complex activity for assessing an information system in order to set forth a qualified opinion regarding the conformity between the system and the regulating standards, as well as over the information system’s capacity of achieving the organization’s strategic objectives, by efficiently using
the informational resources and by ensuring the integrity of the processed and stored data.

**Objectives of Information system audit**

The objectives of IT audit include assessment and evaluation of processes that

(a) Ensures asset safeguarding – ‘assets’ which include the following five types of assets:

1. Data
   
   Data objects in their widest sense, i.e., external and internal, structured and non-structured, graphics, sound, system documentation etc.

2. Application Systems
   
   Application system is understood to be the sum of manual and programmed procedures.

3. Technology
   
   Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

4. Facilities
   
   Resources to house and support information systems, supplies etc.

5. People
   
   Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

(b) Ensures that the following seven attributes of data or information are maintained.

1. Effectiveness - deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner. Deals with System effectiveness – evaluating whether the IT system meets the overall objectives of top management and users.

2. Efficiency - concerns the provision of information through the optimal (most productive and economical) usage of resources. Deals with System efficiency – efficient systems use optimum resources to achieve the required objectives

3. Confidentiality - concerns protection of sensitive information from unauthorized disclosure.

4. Integrity - relates to the accuracy and completeness of information as well as to its validity in accordance with the business’ set of values and expectations.

5. Availability - relates to information being available when required by the business process, and hence also concerns the safeguarding of resources.

6. Compliance - deals with complying with those laws, regulations and contractual arrangements to which the business process is subject; i.e., externally imposed business criteria. This essentially means that systems need to operate within the ambit of rules, regulations and/or conditions of the organisation. For example, an FIR to be filed normally requires signature of the complainant as per rules, and needs to be reengineered by changing the rules to permit web based complaints. Similarly, banking operations will have to conform to the banking regulations and legislation. It is also the duty of the IT Auditor to see that the work practices are in tune with the laws of the land such as the IT Act promulgated by the Government of India.

7. Reliability of information - relates to systems providing management with appropriate information for it to use in operating the entity, in providing financial reporting to users of the financial information,
and in providing information for reporting to the regulatory bodies regarding compliance with laws and regulations.

Thus, IT Audit is all about examining whether the IT processes and IT Resources combine together to fulfill the intended objectives of the organization to ensure Effectiveness, Efficiency and Economy in its operations while complying with the extant rules. This can be depicted diagrammatically as follows:

![Diagram of IT Audit Process]

### NATURE, SIGNIFICANCE AND SCOPE OF SYSTEMS AUDIT

#### Nature of System Audit

It has been the practice in Industry to carry out financial, managerial and technical audits. The oldest and most prevalent audit has been the financial audit. Traditionally, financial auditors have been going by the paper-based book of accounts. They have been focusing mainly on ensuring internal controls and compliances with the laws of the land, and thereby, good governance.

Managerial audit has been focusing on the basic management policies and practices, with the aim of determining whether the enterprise is in good shape, has good processes and has a good feedback framework for managerial effectiveness and performance.

Technical audit has been focusing more on the shop floor details, such as, whether the manufacturing and maintenance functions are performing efficiently.

With the increasing use of computer-based systems in the enterprise, the complexity of systems and risk of errors, sabotage and fraud have increased manifold. In a network setup, a transaction is initiated in a physically different location, posted in the books elsewhere and the management information aggregated from the data viewed somewhere else. Because of the number of agencies involved and the increased risk exposure of mechanized systems, it is no longer sufficient to go by auditing of the book-based accounts. One has to see the vulnerability of the IT setup to external “crackers” and “hackers”.

The nature of systems audit, unlike the other audits, is not restricted to audit of reported items only. It has to take into cognizance the choice, use and risk of technology. It has to look at the realities of business processes and constantly changing legal framework.

#### Significance of System Audit

For any business (for profit or for nonprofit) to survive, it must have an adequate information security system in place. IT audit is important because it gives assurance that the IT systems are adequately protected, provide reliable information to users and properly managed to achieve their intended benefits. Many users rely on IT
without knowing how the computers work. A computer error could be repeated indefinitely, causing more extensive
damage than a human mistake. IT audit could also help to reduce risks of data tampering, data loss or leakage,
service disruption, and poor management of IT systems. Few of important reasons for which system audit is
gaining significance are:

1. Ensuring the security of information
2. Standardization.
3. Improvement in business efficiency.
4. Improved system and process controls.
5. Plan for contingencies and disaster recovery.
6. Evaluating the effectiveness and efficiency related to the use of resources.
7. Reduced risk and enhanced system security
8. Prevention and detection of errors and fraud
9. Building Confidence and Public Reputation

Scope of Information System Audit

The information system of any company has different functions and activities coupled with a number of computer
installations at different geographical locations. There are risks inherent to information systems which may
impact the information system in different ways. The scope of systems audit covers the entire IS management
process. The scope includes review of the entire design & development process, the review of technology
choice, the processes employed to assess risks and losses that could accrue to the system, the possibility of
computer frauds, the care taken in managing changes to the system, extent of testing and reliability of the
system.

The IS auditor is expected to adopt a risk-based approach for making an audit plan. Following are the main
areas of scope for an IT auditor

Report Validation - To provide assurance that the reporting module of the system is working according to the
specification, are error free and can be trusted i.e. Functional Audit of the reports produced by the system,
formulas used for different calculations are in line with industry best practices nationally and internationally.

Application software review - To provide assurance whether the financial and operational applications meet
the current and future needs of the organization. The auditor must access control and authorizations, error and
exception handling, business process flows within the application software and complementary controls (enterprise
level, general, application and specialist IT control) and procedures and validation of reports (both operational
and financial) generated from the system.

Network security review – To provide assurance that the database and the web server system is fully secure
and is corresponding to the controls objectives of control system. Review of internal and external connections to
the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection
are some typical areas of coverage.

Data integrity review - To provide assurance that the database design and structure provides the best possible
design for the organizational needs and corresponding application and future integration needs. The purpose is
scrutiny of live data to verify adequacy of controls and impact of weaknesses, as noticed from any of the above
reviews.

Business continuity review – It includes existence and maintenance of fault tolerant and redundant hardware,
backup procedures and storage, and documented and tested disaster recovery/business continuity plan,
effectiveness of disaster recovery plan, as well as ensuring existence of well defined I.S Audit manual and its compliance thereon.

The IS Auditor must analyze business process risks and controls based on an understanding of planned or implemented controls and identified control gaps. The IS auditor is required to review role of Internal audit in relation to IS audit. This may involve evaluating audit plans and reporting to audit committee and senior management on controls, specific resources required for performing IS audit function.

**STEPS INVOLVED IN CONDUCTING SYSTEMS AUDIT**

The following are the steps in information systems audit:

1. **The preliminary review phase**

   The first step in an IS audit is the preliminary review of the computer installation. The main objective of this step is to obtain the information necessary for the auditor to make a decision on how to proceed with the audit. This stage includes a review of the management and application controls existing in the company. During the review, the auditor tries to understand the management practices used at different levels of the computer hierarchy.

   The main sources of information during this phase include interviews with installation personnel, observations of installation activities, and reviews of installation documentation. Questionnaires, flowcharts, and other databases can also be used to gather required information. Based on the initial review, the auditor takes a decision whether to proceed with the audit or abandon the entire process.

2. **The detailed review phase**

   The objective of this phase is to obtain the information necessary for the auditor to have an in-depth understanding of the controls used in a computer installation. Upon review, once again a decision by the auditor as to proceed with the process or abandon it must be taken.

   On taking a decision to proceed with the audit process, the auditor reviews both the management and application controls. The management controls are reviewed first, as major weaknesses in these controls enables the auditor to abandon the review of application controls. In this phase, the auditor must also identify the causes of loss existing within the installation and the controls established to reduce the effects of these causes of loss. At the end of this phase the auditor must evaluate whether the controls established reduce the expected losses to an acceptable level.

   Like the preliminary stage, the auditor obtains information for conducting the audit from various sources like company databases, interviews with the concerned personnel, questionnaires etc.

3. **The compliance testing phase**

   The objective of this phase is to determine whether or not the system of internal controls operates as it is supposed to operate. The auditor checks whether all internal controls exist and are working reliably. The auditor makes use of both manual sources of information mentioned above and computer-assisted evidence collection techniques to gather inputs for evaluation.

   At the conclusion of this phase, the auditor must evaluate the internal control system in the light of the evidence collected on the reliability of individual controls.

4. **The substantive testing phase**

   The objective of this phase is to obtain sufficient evidence to enable the auditor make a final judgement on whether or not material losses have occurred during computer data processing. The external and the internal auditor express the results of this phase differently. The former expresses his judgement in the form of an opinion as to whether any misstatement of accounts really exists. The latter however, is
concerned with a broader perspective i.e. given the state of the internal control system, have the losses occurred or could they occur in future due to the weaknesses in control systems used to safeguard assets.

The following are the five types of substantive tests that can be used within a data processing installation:

(i) Tests to identify erroneous processing
(ii) Tests to assess the quality of data
(iii) Tests to identify inconsistent data
(iv) Tests to compare data with physical counts
(v) Confirmation of data with outside sources

5. Overall evaluation

Upon substantive testing, the auditor once again has an overall view of the control systems existing within the company.

6. Documentation

On completing the audit process, the auditor prepares a comprehensive audit report giving details of all the phases of review and testing conducted. The audit report also consists of the recommendations of the auditor for improvement in control systems.

SYSTEMS AUDIT & MANAGEMENT FUNCTIONS

If we look at the time-honored management pyramid,
We notice the major role information systems have to play in decision-making across the Management functions. Information systems usually focus inwards and are endoscopic in nature. Information gathering from the external business world is mostly manual or done through disjointed systems such as taking information out of the Internet, etc. The Strategic vision and direction are set based upon the top management’s perception of opportunities. The information feedback from operations and operational decisions flow to help the middle management in its tactical management. The information flow from Tactical Decisions enable the Top Management to assess where the organization is, vis-à-vis its vision and strategic direction.

Systems Audit helps the management to be assured that its feedback loop is healthy and is not likely to miss out on vitally important details. Any deficiencies in the Information systems and in the creation, maintenance and usage of the information are pointed out by the systems audit function. In turn, this also reinforces the Stakeholders’ faith in the basic management processes that are tracked by information flows.

All organizations suffer from fragmentation of knowledge across functions and across departments as well. Paretto’s principle seems to apply well in that 20% of the people get to have 80% of the knowledge of their departmental/functional area. The challenge before all managements is, how to manage knowledge. Knowledge needs to be distributed instead of being hoarded, so that the activities of the company are at the optimal best.

In its primitive form, a Knowledge Management system today is a glorified form of document management system. The extent and granularity of indexing determine how closely relevant a piece of knowledge can be. Raw knowledge has to be validated to make sure that it is well supported by facts. Only then it can be used. Use of invalidated knowledge can be dangerous. Systems are evolving from information management to knowledge management. The traditional management function of planning, directing, coordinating, analyzing and staffing are deeply impacted by information and knowledge.

At a more mundane level, all functional managers need to cooperate with IS Audit so that the exposure of a weakness can be converted into a strength.

**SYSTEM AUDIT OF DIFFERENT FUNCTIONS**

IS Audit is an evaluation of adequacy of controls. In a computerised environment, controls can be classified as under, which are verified by the IS Auditor:

**A. Management Controls**

1. Security Policy and Standards
2. Constitution of Steering Committee
3. Business Continuity Planning
4. Systems Development Methodology

**B. Operational Controls**

1. Monitoring physical assets
2. Ensuring adequate environmental controls such as Air-conditioning (dust, temperature & humidity controls), Power Conditioning (Online UPS functioning all the time with backups, proper earthing)

**C. Organizational Controls**

1. Defining roles, responsibilities and duties of User Departments and IT Department
2. Defining roles, responsibilities and duties within IT Department – such as developers, operators and administrators

**D. Application Controls**
1. Each of the Computer Systems and subsystems must have its own set of controls for Inputs, Processing & Outputs. Processing controls should also ensure checks for legal compliance.

2. While performing the audit, each of the controls needs to be studied for its existence and adequacy.

**AUDIT OF MANAGEMENT CONTROLS**

**Security Policy and Standards**

The IS auditor should first verify whether the organization has a Security Policy. If it does not exist, the auditor needs to point this out, unless the management has a corporate IS Security policy and follows standard implementation of IS Security across all units and divisions.

If a security policy exists, it needs to be examined for currency and adequacy in proportion to the risk. The security policy has to be always dynamically updated.

**Steering Committee for Security**

The formulation and implementation of a sound security policy should not be the handiwork of just the IT Department. It should be a team effort, brought into effect by a committee in which there is at least one member of the Board of Directors apart from the CIO and User HoDs. The auditor should point out the absence of such a committee.

Without such a committee having regular planned meetings with agenda and action points, the implementation of security policy would be in jeopardy. The auditor needs to stress upon the possible benefits of a properly functioning steering committee or conversely, the disbenefits of not having such a committee. In recommending the constitution and functioning of the committee, the auditor should be specific about composition, individual roles and responsibilities and monitoring/escalating mechanism.

**Business Continuity Planning**

Business Continuity is a very important aspect of Information Systems. It encompasses all aspects that can result in usage discontinuity. As a simple example, let us say that a company has three servers connected to a single UPS. The UPS is not under Annual Maintenance Contract. Its batteries may be dying out. Since there is no mechanism to look into the health of the UPS, it can go down without a warning, resulting in a server tripping. All work halts till the UPS can be set right. If such a catastrophe occurs in a remote place, then the time to repair/replace the UPS can be longer.

The IS Auditor should examine all such possibilities by which the availability of Computer Systems is threatened with temporary or permanent breakdown. In sensitive areas, even proofing against mob violence/terrorist strikes should be kept in view.

**Systems Development Methodology**

In most companies Systems Development is badly handled. And proper documentation is not maintained. The code is developed in great hurry and control aspects are given the go by. The accuracy of the processing and the legal compliance are left as open questions.

The IS auditor should verify whether following documents exist or not:

1. Functional requirement Specifications
2. Software requirement Specifications
3. Design Description
4. Software code
5. Test Plan

6. Unit test results

7. Integration test results

8. Acceptance test results

The documentation should be properly cross-indexed. The effect of a change made in the system should be well understood. It should not happen that, due to ignorance of the entirety of the business process and its ramifications, a change made in one area affects other areas, that too after a lapse of time.

Every time a change is made, a thorough testing should be done and documented.

The IS Auditor should get necessary evidence and comment on the lack of proper adherence to procedure.

AUDIT OF OPERATIONAL CONTROLS

The Auditor should observe the operations and comment on the drawbacks. Some of the possible scenarios are:

(a) Anybody walks into the server room and has access to documents/media/machines.
(b) Backup media not labeled properly and kept under lock and key.
(c) One set of backup not regularly kept at another location
(d) No documented and organized change control process. Software and data are arbitrarily changed.
(e) Correction of errors not done by reversal of entry but by running dangerous script on the database backend.
(f) Administrator passwords freely floating around and used by developers, operations staff and administrators.
(g) Dirty network cabling with loose cables hanging around, hand crimped cables, cables not tagged for easy identification.
(h) Switches/hubs lying loose on tables/hanging on walls.
(i) Data controls not properly checked and filed.
(j) Preventive Maintenance of Servers not done.
(k) Machines working with covers kept off.
(l) Media not properly labeled and recorded in media register.
(m) Absence of gate pass culture: machines arbitrarily taken from/into computer rooms.
(n) Unknown and untrusted CDs directly used without checking for virus.

The above scenarios speak of a very casual IT setup. Such carelessness can result in serious downtime. Sensitive data can be pilfered from the servers. The IS auditor needs to highlight these flaws as serious lapses.

Audit of Environmental Controls

The following environmental factors need to be checked and commented upon by the auditor:

(i) Online UPS not used; either line-interactive UPS or Offline UPS used, or CVT used.
(ii) Electrical cabling loose / points having loose contact.
(iii) No separate earth pit for the Computing equipment.
(iv) Switches/Hubs/Routers not fed UPS power.
(v) Server room door kept open.
(vi) AC not functioning properly, especially in summer.
(vii) In winter AC set at 29 Deg C instead of 22 Deg C.
(viii) No pest control measures taken.
(ix) Eatables taken into server room/ Smoking in the server room.
(x) Heavy duty printer kept inside server room: scope for dust.
(xi) UPS, AC, other electricals not under regular AMC.
(xii) No genset backup in case City power supply fails for long hours.
(xiii) No smoke detectors/fire alarms in server room area.
(xiv) Fire extinguishers not kept filled and ready.
(xv) No fire drill carried out to make people aware of dos and don’ts

The above are serious lapses that can seriously affect the functioning of the IT Setup and cause work stoppages.

**AUDIT OF ORGANIZATIONAL CONTROLS**

There needs to be an effective Organization Chart for the IT function. In some Organizations, IT is treated as a technician's job. A very junior person is made the head of IT. He/she will be unable to hold his own when powerful functional heads as the Finance Head or the Production head keep breathing fire. It is best to have the IT function reporting to the CEO. The Head of IT is the Chief Information Officer or CIO.

The CIO should have three reportee managers – one for taking care of the development team, one for ensuring Information System / IT Center security and another for managing the facilities (i.e., operations and maintenance of hardware, OS, database administration, vendor management, service providers, etc.) It is advisable not to club IS security with operations or development.

The IS auditor should look for a succession plan for the IT Management team. The main concern here is that a few persons may be knowing the ins and outs of the software. They may be fixing problems because of their deep knowledge of the code. Other than in their minds, there is no documentation of what they know. Either because of their leaving the organization or their disgruntlement, they may not keep doing the good work. Such an event would compromise the functioning of the systems and emergent solution to the problem may be very expensive.

The IS Auditor should check for clear-cut definition of User role, IT Role so that there are no ambiguous overlaps. For example, it should be clear that the Wage Administration section would advise tax rate changes, etc. to the development and maintenance team member concerned. Under the formal authorization of the user HoD, such changes should be carried out. Deciding which data should be kept and which should not be kept is the responsibility of the User and not IT Department. Making a final pronouncement on the correctness of processing by software is again the concerned User Department responsibility.

There are companies in which there is no specific duty allocation to IT Staff members. This is not desirable, since everybody escapes accountability. One section of IT Department must take the responsibility for developing and maintaining the software. They should have nothing to do with the Hardware upkeep, System, Network and Database administration. This should be looked after by another set of people. Systems security was earlier the purview of the system administration staff. Given the increasing dependence on computer systems and the ever-increasing security risks, it is necessary to ensure that no person who has executive responsibility should have anything to do with an audit type of function. This is the reason why Security and Audit of systems should
be the responsibility of a different section. This group needs to have a very good technical knowledge of IT and security risks. It would only audit and report findings to the management without getting into actual solution implementation. Any deviation in this regard needs to be pointed out by the IS Auditor, including an impact analysis.

**SYSTEMS AUDIT OF COMPUTERIZED SECRETARIAL FUNCTIONS**

The procedure to be followed for performing a systems audit remains the same irrespective of functionality. Only the testing of application controls varies for audit of different functions.

**Application controls**

These are manual or automated procedures that typically operate at a business process level and apply to the processing of transactions by individual applications. Application controls can be preventative or detective in nature and are designed to ensure the integrity of the accounting records. Accordingly, application controls relate to procedures used to initiate, record, process and report transactions or other financial data. These controls help ensure that transactions occurred, are authorised and are completely and accurately recorded and processed.

In relation to system audit of computerised secretarial function, Application controls apply to data processing tasks such as feeding shareholders details, directors details, date of meeting, details of agenda items etc. and are normally divided into the following categories:

(i) **Input controls**

After verifying the system development methodology, the secretarial audit should verify the input controls in the systems and procedures developed for computerized secretarial function.

The input will consist of the details of the various shareholders. The Master Data would contain the name, address, nominee, or joint account holding details, as also income-tax status. Before the Dividend Warrant application program could be run in a live environment the steps that would be taken would be to ensure all master records have been corrected, upto and including Share Transfers as approved by the last Share Transfer Meeting, and also all correspondence received regarding change of address, income-tax status etc.

The first and initial input control would be to run the data file of the shareholders and obtain the total of the shareholding to ensure that it is equal to the subscribed share capital. An error at this stage would indicate that some wrong corrections have been made to the Master Data like the transferee details would have been included and the transferors details might not have been deleted or when a transferor has effected a part transfer, suitable corrections might not have been effected.

(ii) **Processing controls**

An example of a programmed control over processing is a run-to-run control. The totals from one processing run, plus the input totals from the second processing, should equal the result from the second processing run. For instance, the beginning balances on the unpaid dividend ledger plus the dividend declared ledger (processing run 1) less the dividend paid (processing run 2) should equal the closing balances on the unpaid dividend ledger.

(iii) **Output controls**

Batch processing matches input to output, and is therefore also a control over processing and output. Other examples of output controls include the controlled resubmission of rejected transactions or the review of exception reports (eg the list of directors reports showing the name of director who is debtors of more than Rs 1 lakhs of the same company).

(iv) **Master files and standing data controls**
Generally, every time after the Share transfer Meeting, the Master file of the Shareholders would be modified to take into account the latest changes in shareholdings. General practice that could be followed would be that at every point of time it would be ensured that the Master File contains the correct total figure of shareholdings. When modifications have to be made because of the authorized share transfers, there would be a separate verification program to ensure that the number of shares transferred by the transferors is equal to the number of shares transferred to the transferees.

So, when performing the Systems Audit, one must verify these records to ensure whether all these procedures have been followed. It is not uncommon to hear of stray incidents when transferor and transferee might have received dividend warrants or the transferor receiving the dividend warrant and not the transferee! In those circumstances, while the computer is conveniently blamed, the real culprits are the individuals who are not following the procedures correctly. In a manual environment, before the procedure of computing dividend warrants is commenced, it is manually ensured that all of the transfers as per the list as authorized by the Directors have been correctly posted. The same procedure needs to be verified in a computerized environment. As we would not be verifying the manual posting, a computer program is run to ensure the integrity of the Master file of the shareholders.

### NORMS AND PROCEDURES FOR COMPUTERIZATION

Computerization often known as automation is very important for an organisation. In present scenario, automation of information system has become an essentiality and without automation, it is very difficult to run an organisation. In this section of study, we will discuss about norm of automation and its procedure.

Automation refers to the use of computers to manage the administrative and information processing tasks in records offices, records centres, and archival institutions.

If used wisely, computers can assist records personnel in managing records better to ensure their continued value as evidence. Automation can help organisations implement authentic and reliable record-keeping practices, through the improved tracking of records through their life cycle as well as the consistent application of records schedules and descriptive standards. Maintaining evidence through authentic and reliable records is a cornerstone of good business practice and helps ensure a valuable record for society.

### What Should Be Automated?

The range of technology applications and functions available can make it difficult to select a particular technological solution to a records or archives problem.

The question is not whether records and archives management functions can be automated. Many functions can be automated if the resources are available. But it is important to determine if automation is warranted. Two key questions must be asked:

1. Should a specific records or archives management function be automated at this time?
2. How should a particular records or archives management function be automated?

All records and archives functions should be fully functional in a manual system before attempts are made to automate them. Automating an inefficient process will not transform it into an effective one. If done correctly, however, automation can not only improve archival and records functions but can also make it possible to undertake activities that were too complicated or time consuming to be done in the past on a regular basis.

All records and archives functions should be fully functional in a manual system before attempts are made to automate them.

Because automating an inefficient and ineffective manual process will not help an organisation achieve its objectives, some organisations should consider systems analysis and business process re-engineering in anticipation of automation.
**Business process re-engineering (BPR):** The fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service and speed.

It is also important to consider the resources available and staff commitment required before commencing an automation project. Financial resources are important, but people are an even more critical element in any automation process. When considering automation, the key stakeholders need to be identified.

**Stakeholder:** Any person, group or other organisation that has a claim on an organisation’s attention, resources or output or is affected by that output.

These stakeholders may include government officials who rely on the archival institution to maintain their records and supply information or return specific files when requested. Other stakeholders are the citizens who depend on the records and archives institution to be able to preserve and locate important records (such as property files) and the staff of the records and archives institution. Researchers may be another key stakeholder group; they can be directly affected by the way information or records are made available to them.

Whether an automation programme succeeds or fails often depends on the support it receives from stakeholders. Automation may entail redesigning work processes and thus changing people’s jobs or the way services are offered. It is crucial to assess people’s capacity for change in their work environment and to prepare them for that change. Staff may have to be trained in computer skills. Similarly, users may have to be given guidance about the way automated systems work if they are to be expected to use the technology themselves.

### Reasons for Automation

Automation should be viewed as a tool to facilitate daily operations and planning in a records and archives institution. If implemented well, automation can increase staff efficiency, perform routine tasks automatically and analyse data more quickly than could be done manually. Manual information systems may not be fast enough or sophisticated enough to meet growing user demands as well as the higher expectations and standards brought about in society by increased computerisation. If people find that they can access information in one office or agency using computers, they will soon come to expect other offices to provide the same level of service.

Public and private sector organisations increasingly rely upon computers and information technology to deliver their services and programmes more efficiently. Records and archives institutions are not exceptions to this trend. Almost any records-related activity can be automated in some fashion. For example, word processing can be used for correspondence, inventory development and report generation. Spreadsheets can be used to manage budgets or track project expenditures. Databases can maintain information about staff or about records or archives.

**Automation should facilitate daily operations and planning.**

The pressures to automate are great. In this age of ‘instant’ information, there is an increasing demand for speedy access to information, records and archives. Furthermore, existing manual systems may lead to duplication of effort and repetition of work. Manual systems can be time consuming, costly, inflexible and prone to human error. However, as will be discussed below, computerisation is only effective if the proper analysis and planning is completed prior to the purchase and implementation of new technology. Computers alone are not a solution for poor processes or a lack of standards in the management of records or archives. For example, a computer cannot be a replacement for, or an alternative to, a properly designed classification system. On the other hand, if such a classification system is in place prior to computerisation, the computer can automate it, facilitate access and provide a faster search mechanisms for it and permit the assignment of relevant file numbers to paper records quickly and efficiently.

Following are some reasons an organisation might choose to automate its records or archives functions, or
Indeed any of its functions.

- accuracy of information and calculations
- speedy retrieval of information
- reliability of information once input
- increased ability to manipulate data once input
- ability to ensure greater accuracy and consistency in the performance of routine tasks
- large capacity for storage of information
- accessibility of information
- expandability of computer systems
- flexibility of computer systems
- cost efficiency of operations
- better utilisation of personnel
- savings in space and equipment
- instantaneous updating
- multiple simultaneous access to information
- new approaches to work processes.

Automation also assists in eliminating repetitious work, such as typing new file labels and index cards. Computers can print labels automatically, update indexes regularly, produce reports based on data already entered into the computer, and otherwise reduce time and increase efficiency. Personnel can then focus their work on more significant tasks.

The computerisation of some tasks offers much more flexibility. For example, the computer makes it possible to organise and maintain an index with several searchable ‘fields’ or attributes of information. As a result, the computer provides increased points of access to information. This access can facilitate the location of items for users who may not be aware of the exact terminology for an item.

**PROCEDURE OF COMPUTERISATION**

**Assessment and Planning**

Planning is a critical management function that must occur within the organisational context; that is, other organisational components must be taken into account while carrying out any planning exercise. In other words, automation projects cannot be planned for in isolation from the organisation’s mandate, mission, functions, resources and other systems.

The computerisation of work processes also requires knowledge, skills and wisdom from more than one discipline. Any automation project has a greater chance of success if it begins with good planning and with consultation with the user and the technology communities, with programme managers, records managers, archivists and systems specialists, as well as with other government officials who depend on records. A system that does not meet the needs of users is counter-productive and represents a misuse of resources. An automation project can only be successful if all stakeholders are involved and, particularly, if senior management supports, endorses and leads such an initiative.

The goals and purposes for automating the records management system should be clearly stated by senior
management and communicated to employees. Future users of the system should be consulted to seek their expertise and ideas and promote their acceptance of the new tool. Training and orientation in the new tool is also critical to its success.

Planning ensures the project is completed on time and within budget and that the final product addresses the needs of the organisation as identified. Planning can be quite complex, but it is a necessary part of an automation project. Without planning, the systems developed may be inadequate, people may be poorly trained and the final project may not be successful. Planning involves

- conducting an initial assessment
- developing goals, objectives and priorities
- determining resource needs
- getting support for the project
- conducting a feasibility study
- developing a detailed project plan
- assembling a project team and project structure.

**Conducting an Initial Assessment**

Whether manual or automated, systems exist within an organisational framework and therefore must be organised in order to meet the needs of the organisation. Prior to developing the automation project in depth, it is wise to conduct an initial assessment of the organisation, to determine if an automation project is in fact even viable. A number of technology-specific factors should be identified and evaluated during this initial assessment phase, including:

- the problem(s) to be resolved by the development of a new automated system
- how technology initiatives fit into overall mission and business objectives
- current or pending legislation that may affect the choice or use of technology
- the state of existing systems within the organisation and how they should relate to any new system
- the system of managing materials in agency records offices as well as in the records centre
- the nature of any existing or planned records management initiatives within the organisation and how they affect or should co-exist with any new system
- the expected benefits resulting from the implementation of an automated system
- how costs will be measured and at what point the costs will outweigh the benefits
- the constraints and limitations of the automation project, including policy, financial requirements and technical skills
- the time and resources required to conduct a feasibility study
- the level of senior management support (it is best to seek a champion for the records system automation project to offer support at senior levels)
- the project team members, their roles and responsibilities.

Once this initial assessment has been completed, it is possible to determine the goals, objectives and priorities for the project and develop the terms of reference for a feasibility study.

Other non-technical factors can affect the feasibility of an automation project. These factors might include the
organisational culture and the physical layout or environmental conditions within the office. Work practices and office cultures will influence the design and implementation of both computer hardware and software. Failure to understand the organisational culture in may result in barriers during the implementation of any automation project. For example, re-engineering a process may entail reorganisation of tasks, additions of duties or deletions of certain steps. This process can affect behaviours and office routines that have been in place for years. If the new automated processes do not work well, they may be of little value because the older routines will persist. In this case, senior management should stress that the re-engineering is not being done for the benefit of automation. Rather, changes are being made to further the goals and objectives of the organisation.

Several physical factors can assist or impede the automation process, including the actual physical layout of the office, environmental issues and infrastructure. Computers and peripherals require large amounts of workspace to create an efficient working environment. Also, computer users can experience muscle pains if office furniture does not support parts of the body, such as the back and arms. Poor alignment between the computer monitor and the line of vision can result in neck problems. The potential for these concerns needs to be identified during the assessment.

The physical environment is also a factor. Consistent temperature and relative humidity must be maintained to ensure proper functioning of the computer technology. Furthermore, computers are also sensitive to excessive dust or dirt, and air conditioners will help to filter the air. Computer technology also relies on dependable power supplies, without significant surges or long-term power cuts. The initial assessment must address these issues as well. Preservation issues are discussed in more detail below.

### Developing Goals, Objectives and Priorities

If the initial assessment proves favourable toward further exploration of automation options, the scope of the project needs to be established. Any automation project (or indeed any project in the organisation) must be well planned, based on clear and achievable goals and objectives and well-established priorities.

If the records management automation project does not blend well with the parent organisation’s overall business goals, objectives and priorities, there is likely to be little support for its development. For example, if someone in a records office wished to develop an automated retention and disposal schedule at the same time as all classification systems were being revised, management may reasonably feel the automation project is premature.

When considering how automation in the records and archives institution will support the organisation’s business objectives and priorities, consider the following issues.

### Purpose of the System

The purpose of records and archives management systems must be phrased in terms of the larger organisation. Records professionals may want to clarify the purpose of the automated system, what other functions it could or should perform and what information is needed within the system. However senior management will want to know the business objectives to be supported by the automated system.

Automated systems must serve the purposes of the larger organisation.

### Technical Considerations

During the assessment and planning process, it is important to consider the organisation’s capacity for maintaining the system and its ability to provide the training necessary to support the use and application of automated tools. This process entails working with individuals responsible for information technology in the organisation and understanding their procedures, policies and areas of expertise. Some questions to consider in this area include the following.

- Is there sufficient technical support to solve hardware and software problems in a timely manner?
– What types of software are supported by the institution?
– What systems are already in place?
– How will the new system work with existing systems?
– Are policies and procedures in place for backing up data on a regular basis?
– What precautions are in place to combat viruses?
– What type of training is offered internally to assist employees in gaining and developing their own computer skills?
– Is there someone close by who can answer questions about software packages used by the organisation?

Organisational Factors

Goals, objectives and priorities for the automation project will differ depending on who in the organisation is involved. A key decision to be made is to determine who should be involved in the automation decision-making process. Other major organisational decisions include the following.

– Who will be authorised to enter, change and delete data?
– Who will have access to view data in the new system?
– Are different levels of access needed in the system?
– How will the new system be implemented (for example, full automation of one records office or incrementally by introducing one computer into a number of records offices)?
– Will it be implemented all at once or in phases?
– What levels and types of training are required for different staff members and other users to understand and utilise the system?

Resource Requirements

Resources are measured in terms of money, time and people. The major question usually is: what will the system cost? However, an expensive system may provide few installation and implementation problems and in the long run be less costly than a less expensive system that is difficult to install, hard for records centre staff to use and shuts down periodically.

An equally important question to ask is: what will be the benefits? This should be answered in terms of the immediate office as well as in terms of the business goals of the larger organisation. Other resource questions include the following.

– Where will necessary funds come from?
– When is the system to be installed?
– Are there sufficient funds to work within this time frame?
– Do sufficient funds exist for long-term maintenance of the hardware and preservation of the data in the system?
– Is there sufficient space to install such a system?
– What are the human resources requirements?

Political Issues

Software designed for automated records management systems includes assumptions about the value of records,
the extent to which it is acceptable to provide access to records, users’ interest in accessing records and the capacity of the economy to afford the technology. Automating records systems may be well received if a government or organisation values accountability, efficiency, effectiveness and economy; they may be poorly received if the government or organisation is not aware of the importance of good records care. Questions to ask include the following.

– Does senior management accept the value of records as evidence?
– Does senior management see the need for the automated system?
– Will management provide financial and organisational support for the programme over the long term?
– Are there any potential champions of the project among senior officials?
– Who must be involved?
– Who should be involved?
– What consequences will acceptance or rejection of the proposal have on the organisation and its departments?

The answers to these questions will help organisers of the project to develop a written statement of goals, objectives and priorities. This statement will form the basis for the organisation and implementation of the automation project. A sample statement of goals, objectives and priorities is presented in the figure below.

In this example, observe that the goal is two-pronged. The records office desires to standardise descriptive data to enhance their own management of records and it wants to make some of this information accessible to users. The two parts of the goal are presented in more detail in the objectives. However, the top priority is to increase managerial control over records through standardisation and creating an easily updatable database. User access is secondary and will be phased in over the course of the automation project. This is not to say that user access is not important. However, objectives must be balanced in a realistic fashion taking into consideration the five areas discussed above, the purpose of the system, technical considerations, organisational factors, resource requirements and political issues.

A written statement of goals, objectives and priorities will form the basis for the organisation and implementation of the automation project.

Computers Control and Security

With increasing dependence on computers, the risk of breach of System security is also increasing. The rising stakes often tempt people to defraud organizations and get away with criminal gains.

If there is no control on printing of Dividend Warrants in the system, an investor could walk away with multiple dividends for the same amount invested. A vendor could get away with multiple payments for goods delivered once. Customer dues can be conveniently whitewashed. Insiders in collusion with external elements perpetrate most of the frauds and share the spoils.

The first principle of control lies in controlling access to the computer system. Nobody should be allowed direct access to the servers other than authorized administrators. Access to the server room can be controlled through swipe-card, fingerprint and other biometric devices. In sensitive data centers, there are movement-sensing cameras that constantly carry out surveillance. Security officers watch the displays in each zone and act when suspicious activity occurs. The key areas are network control area, server bay, power supply, air-conditioning and security control room. Each zone has remote-lockable doors acting as “man-traps”. An intruder can be restrained in the forbidden zone till security officers can nab the person. Modern data centers are also built with flood-proofing, fireproofing and earthquake-proofing measures to ensure that even accidentally through acts of God, the crucial systems are unaffected.
Logical access should be limited to the role played by the user. For example, a data entry clerk need not have access to the Payroll Database. S/he needs only a Read-Write-Update access to the raw data files that can be tracked to the operator. An Accounts clerk need not have access to production data logs.

In order to ensure that the access rights are properly followed, we have the system of passwords. The System Administrator assigns access rights to the users as required by their work. The user protects his/her access through passwords. Ideally, passwords should be minimum 12 characters long, having a combination of letters and numerical digits. Where permitted one can use special characters also. There are cases where users cannot remember their passwords. So they write the password on Post and paste the same on their machines. Or else they use easy to guess words such as their own names or name of wife/child/pet. Such words are usually small and can easily be broken into.

The computer system remembers our passwords by storing them in internal, encrypted files. An expert cracker can retrieve the password if the Operating System has not been set up for the highest security levels.

For example, let us say that a security breach occurs in Microsoft Windows 2000 Operating System. This is reported to Microsoft and they issue an immediate “hotfix” or patch to the OS software that prevents the security hole from being misused. Later on, Microsoft collects similar corrections and bug fixes into a “Service Pack”. Details of such Hotfixes and Service Packs are available in Microsoft’s web site. Users can download such patches and correct their OS. Similarly there are other resources for correcting Unix bugs. When such patches are applied and the recommended security steps are taken care of at the time of the operating system installation, we say that the OS has been “hardened”.

Another class of insecurity comes in through Viruses. Computer Viruses are malicious programs capable of replicating themselves and destroy data or annoy users with meaningless messages. There are malicious codes known as Trojans that can seep into the system through electronic mail attachments. They can remain in the server and copy critical and secret information such as email addresses of others, passwords, credit card numbers, etc. and transmit the information to their creators. In turn the creators can indulge in frauds or cause trouble by changing the password, etc.

Internet web sites are attacked by different methods. The Denial–of-Service (DoS) attacks essentially flood the web server by sending thousands of high priority system messages. The server is rendered too busy responding to such spurious messages than attending to productive work.

In “spoofing” attacks, the user is deluded to get into some unwanted site by overriding the Domain Name Service entries. It needs to be remembered that information travels in packets that have the destination IP address. All computers in the network receive all the packets though they respond only to packets destined for them. A hacker or cracker can use this information to recraft the information content in the packet.

Modern information systems are used to connect external agencies such as service providers, customers and suppliers to the internal network through the medium of Internet. This is where the major risk lies.

Networks are protected from attackers by using:

- Appliances or software called “Firewalls” which restrict entry to outsiders based on security policy.
- Content Inspection & Intrusion Detection Systems, which monitor incoming packets and look for known or suspicious attack patterns. When they encounter suspicious code, they block the packets containing the same and thus protect the server.
- Antivirus software that is kept up-to-date with latest viral identities so that infected files can be identified and quarantined if not cured.

Organizations require security experts to keep a constant watch on network security as attack patterns are dynamically changing. Recent studies by the FBI have shown that most of frauds and damages have been done with insider collusion. Hence one needs to watch activities within and without.
Security of Information in transit over the network is taken care of by encryption, secure tunnels and tracking.

Encryption basically consists of transforming the information from an intelligible form to a non-intelligible form while sending. While receiving, the received information is transformed back to the original form. Modern encryption uses a pair of keys, one called “public” which is downloaded to the sender on initiation of the session. The sender’s machine uses a mathematical algorithm to encrypt the information. This encrypted information can only be decrypted with the “private” key, which the receiver has, on his/her machine. Thus even if a cracker traps the information, s/he cannot decrypt it. It is no use trying to decrypt by permutation because not even the fastest of computers can crack the encryption in years of continuous working!

Secure tunnels are established by a combination of encryption and authentication by a special signature. Tracking tools are available to monitor the entire path taken by the transmitted information. In the event of suspicious activity, the offending machine can be identified and reported.

A major concern in carrying out commercial activities over the Internet or any public network is “repudiation”. For instance, a person A buys some goods online and feeds his/her credit card number. When the card company presents the bill, A can refute it, saying that the purchase was not ordered by him/her and that it is the case of misuse. Modern technology offers methods by which the sender can be uniquely identified and it can be established that the order was, indeed, placed by A. This is known as “non-repudiation”.

Computer Security is a very technical and complex subject. An IS Auditor needs to be aware of the type of attacks. S/he should know the various risks and consequences. S/he should verify whether there is a security policy in the organization and whether there is a mechanism to keep it up-to-date.

The IS Auditor should also verify whether passwords are being properly constructed and kept safe. The Systems Administrator should be aware of the security risks and their mitigation. This is what can be commented upon by the IS Auditor if s/he sees a gap.

### TESTING OF COMPUTER SYSTEMS – DOCUMENTATION STANDARDS, POLICIES AND PROCEDURES AND AUDIT APPROACH

#### Documentation of the system

Systems documentation normally takes the form of narrative descriptions, flowcharts or a combination of the two.

#### Narrative Descriptions

A narrative description helps to give a complete picture of the system. It provides a detailed record of the system under audit and, taken together with other forms of system records, it should cover:

1. System objectives and targets;
2. Links and interfaces with other systems;
3. The environment in which the system operates;
4. The allocation of authority and responsibility;
5. All key controls and systems processes;
6. Exceptional situations or cases that may need to be dealt with by the system;
7. Ad hoc controls such as management reviews.

Narratives may cover detailed descriptions of transaction flows but in some cases these can be better recorded through flowcharts. It is often useful to use a combination of narratives and flowcharts – using flowcharts to describe more complex parts of the system. If flowcharts are used as well they and the narrative descriptions
should be cross-referenced to each other.

Narrative descriptions may be usefully divided into:

- A summary overview of the system; and
- Separate detailed descriptions of the main constituent parts of the system.

Full use should be made of headings and they should be organised in a logical way in order to give a clear picture and make handling and updating easier. Wherever possible the source of the information and the names and titles of people interviewed should be recorded. A clear concise record of the system should be prepared.

**Flowcharts**

Flowcharting is a diagrammatic method of recording and describing a system, which shows the flow of documents or information and the related internal controls within a system.

Flowcharts can help:

1. To obtain a perspective on the whole system;
2. Gain an understanding of the auditee’s objectives;
3. Identify segregation of duties;
4. Help the person supervising the audit to identify areas which are not being covered by the audit.

Flowcharting is likely to be most effective if a logical, top-down approach is taken by starting with an overview or summary flowchart, followed by detailed flowcharts of specific processes if necessary.

There are various methods of, and symbols for, flowcharting.

When preparing flowcharts remember:

(a) Flowcharts are primarily designed to show document flows rather than operations – although other operations can be explained by means of narrative notes if necessary;

(b) Try to avoid mixing up the ‘regular’ process and exceptional processes (two or three transactions per period) on the same flowchart. Prepare separate charts for the regular and the exceptional processes;

(c) To consider whether it is better to record the system by preparing one or more basic flowcharts which show the main flows in the system - supplemented by narrative description where necessary;

(d) To flowchart the actual system. In some cases it may be necessary to record the ‘official’ system, and in those cases the charts must be labeled clearly to show whether it is the official (prescribed) or the actual (real functioning) system;

(e) To work in pencil. This will save time redrawing the flowchart when you make a mistake;

(f) That each flowchart should have a title, the date of creation and of any amendments to it and the name of the person who drafted it;

(g) To make sure that all documents (and every copy of each document) on the flowchart are fully dealt with;

(h) To think carefully before preparing a flowchart. Ask yourself whether it’s really necessary or whether narrative description will be just as effective and less time-consuming.

Flowcharting can be a very effective way of recording document flows in a system.

Advantages of flowcharting are:
• Information can be easily communicated and assimilated;
• Flowcharts highlight the relationship between different parts of the system;
• The auditor can see the whole flow of documents: potential bottlenecks can be identified easily;
• Flowcharts offer a consistent method of recording;
• The auditor has to obtain a clear understanding of information flow in order to draw up a flowchart of a complex system;
• Cross-referencing between systems is made easier.

There are a number of disadvantages to using flowcharts. The most important is the time they can take to prepare. It is very easy for auditors to spend a lot of time preparing a flowchart when it would have been more efficient and useful to do a narrative description instead. Other disadvantages are:

• They are limited in scope and may not identify managerial and organizational controls;
• The technique and conventions have to be learned and practised;
• Complex flowcharts may confuse rather than clarify;
• The auditor usually needs some training and experience to be fluent in preparing them.

**Organisation Charts**

The organisational structure relating to the system under audit should be recorded. A copy of an existing organisation chart will suffice, as long as it is accurate and up to date.

An up-to-date organisation chart will show details of the information flow, relationships in the organization and responsibilities. It is also useful in identifying staff and deciding where audit testing needs to be done. The date the chart was prepared should be recorded.

The chart may include:

• Main department/units with a description of their functions;
• Job titles, grades and names of staff together with lines of responsibility;
• All reporting lines.

**Minimum Contents of System Documentation**

Whichever method is used for documenting the procedures in each system there are certain items, which should be included on every system file. These are:

• Examples of documents describing their purpose and use. These documents and reports should be filed in the order in which they are used in the system, and cross-referenced to the narrative note or flowchart.
• Examples of reports (whether computerised or manually prepared) describing their purpose and use;
• Details of the number of transactions passing through the system. These are essential to a full understanding of the context of the system in relation to the overall activities of the entity. It is therefore necessary to summarise data such as:
  (a) Number of transactions;
  (b) Value of transactions;
  (c) Seasonal fluctuations.
It may also be useful for the auditor to know the number of employees or a stratification of the transactions by value or age to assist in the evaluation of risk when a weakness is highlighted.

The Documentation Standards have been touched upon in the section on Change Management. Documentation guidelines are decided by policies.

In the Audit Approach, an IS Auditor goes through the documentation to understand the system and the controls provided for. The IS Auditor may get clues from other audits such as Financial audits to focus on areas that need attention. S/he then prepares specific test cases, which are passed through the Computer system. Deviations are noted down and covered in the report.

Importantly, the IS Auditor looks at the standard of documentation. Is it clear? Is it Current? Is it complete? An example of Documentation Standards for the Data Model approach is given as Annexure A.

**ANNEXURE A**

**Title Page:** It should contain a general description of the System, the areas it covers and the areas it does not cover.

**Documentation:**

1. **Requirements Documentation:** The purpose of the requirement section of the documentation is to define the problem so that the solution can be planned.

   1.1 **Name – Short title is given**
   - Problem statement – State what needs to be done, e.g. Share Capital needs to be updated after each transfer meeting.
   - Problem Illustration – Complete and detailed specification of the problem should be given. Any assumptions made regarding the problem should be stated. This should provide a real world description of the problem, its input, its output and its processing.

1.2 **Input Information**

   1.2.1 **Input Files (to repeat for each input file)**
   - Name
   - Description – how is the file used?
   - What is the purpose?
   - Format – How are the data organized and formatted?
   - Size – What is the expected number of lines (or records or items)
     - Is the number fixed or variable? If variable, is there a minimum or maximum?
   - Sample – provide a sample of properly formatted input.

1.2.2 **Input Items: Repeat for each data element or program input**

   - Description – What does the input or data element mean?
   - Type – What is its logical data type (e.g. integer, alpha-numeric etc.)
   - Range of acceptable values – What is the acceptable range for this program
1.3 Output Information

1.3.1 Output files (repeat for each file or stream)
- Name
- Description – How is it used? What is its purpose?
- Format – How are the data organized and formatted in the output file
- Size – How many number of lines (records or items) are accepted
- Is the number fixed or variable? If variable, is there a minimum or maximum.
- Sample – provide a sample of properly formatted output.

1.3.2 Output items: Repeat for each program output
- Name
- Description – What does the output element mean? What is it used for?
- Type – What is its logical data type (integer, alphanumeric)
- Range of Acceptable Values – What is the acceptable range for this program.

1.4 User Interface Information
- Description – How will the user interact with the program?
- Types of user interfaces include menu selection, Form Fields, command language etc.
- Sample – include illustrations of screens.

1.5 Specifications: Description of functionality

2. The purpose of section of the documentation is to describe the plan for the solution of the problem. The software system consists of all components of the software product. The components are a collection of related items (sub-routines, constant etc.)

2.1 System Description: This section includes a list of each system component.

2.2 Component Information: A solution will include several types of system components. It consists of:
- Data abstraction
- Functional abstraction.

Module Information (repeat for each module)
- Module Name – Name of the Data abstraction
- Descriptions – briefly describe the task it performs. Specify accepting inputs and outputs

Data Abstraction Attributes – repeat for each attribute.
- Name
- Description
- Type
- Range of acceptable values.

Data Abstraction operations —
Functional Abstraction Components: Functional abstraction components consist of collection of sub routines that work together to carry out a portion of the requirements of the overall system. All sub-routines other than the main routine and those listed in the section on audit abstraction components should be covered in this section.

Sub Routine Information:
- Name
- Brief description of its function
- Input parameter – Name, type and purpose for each parameter
- Output parameter – Name, type and purpose for each parameter.

Design diagrams: Diagrams should be used to illustrate the design.

Structure chart is a true diagram of the sub-routine in a program. It indicates the interconnection among the sub-routines.

Pseudo Code – This section should describe in an easily readable and modular form how the software system will solve the given problem. Using simple Standard English terms, there should be a description of the problem and how exactly the solution is obtained.

III. Implementation Document: The purpose of this documentation is to give details of how the system has been implemented.

Physical Organization of System Components: Different components of the System. The architecture will appear in different compilation.

Comments: The program design information should be explained. It should broadly cover System Documentation, Problem Statement, Problem Specification, System Architecture.

Programming style: Programming style refers to those conventions that enhance the readability of the program.

IV. Verification and Validation Documents: The purpose of the verification and Validation documents is to demonstrate the operation of the program, describe how it is run on the machine and present evidence of program verification and validation.

IV.1 Planning
- Approach – What is the approach which has been adopted to ensure system software works correctly.
- Test Cases and Test Audit include a list of input data that test thoroughly the logic of the program and demonstrates that the program satisfies its requirements. If each of the test data explain the requirements it will exercise.

IV.2 Outcome of Verification and Validation
Summary of verification and validation results: Give a brief description of the results from your verification and validation activities.

Verification and Validation Process: Provide a description of the procedure followed and any changes made.

IV.3 Operating Directions: The name and version number of the compiler used
– Name and location of the version program file, executable file, and any data files used.
– Names and locations of different files which are needed to be compiled to execute this program.

IV.4 If the program has any bugs that needs to be indicated. Explain what parts of the program work and also any caution that needs to be exercised to avoid problems.

V. Version History
– Revision I
– Revision II
– Original Version

LESSON ROUND-UP
– Information systems auditing or systems audit is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently.
– The objectives of information system audit include verifying safeguarding of assets, data integrity, system effectiveness and system efficiency.
– To start system audit, a plan has to be developed, covering scope and objectives, key strategies for Analysis and understanding of standard procedures, Evaluation of system and internal controls. Audit procedures and documentation of evidence etc.
– Information systems auditing is not just a simple extension of traditional auditing. The discipline of information systems auditing has been shaped by knowledge obtained from four other disciplines i.e. traditional auditing, computer science, behavioural science and information system management.
– The nature of systems audit, unlike the other audits, is not restricted to audit of reported items only. It has to take into cognizance the choice, use and risk of Technology. It has to look at the realities of business processes and constantly changing legal framework
– The scope of systems audit covers the entire IS management process. The scope includes review of the entire design & development process, the review of technology choice, the processes employed to assess risks and losses that could accrue to the system, the possibility of computer frauds, the care taken in managing changes to the system, extent of testing and reliability of the system.
– IS Audit is an evaluation of adequacy of Management controls, Operational Controls, Organisation controls and application controls.
– Steps involved in conducting IS audit includes, purviewing of the environment, Understanding the Information Systems, Identification of the Audit Risks, Audit Evidence, Key Control Points and Identify Control Weaknesses, Verifying veracity of computer files, Conduct Audit Tests, Concluding the Audit
– Collecting evidence on the reliability of a computer system is often more complex than collecting evidence on the reliability of a manual system. Auditors confront a diverse and sometimes complex range of internal control technology that did not exist in manual systems. Auditors must understand these controls if they are to be able to collect evidence competently on the reliability of the controls.
– Given the increased complexity of computer systems and internal control technology, it is also more difficult to evaluate the consequences of control strengths and weaknesses for the overall reliability of systems. First, auditors must understand when a control is acting reliably or malfunctioning. Next, they
must be able to trace the consequences of the control strength or weakness through the system.

-- For doing the system Audit of Computerised Secretarial Function, the auditor should note that the procedure to be followed for performing a Systems Audit remains the same irrespective of functionality. The testing of application controls alone vary. Systems audit consists of evaluating the Management Controls, Environmental Controls, Organizational Controls and Application Controls

---

**SELF-TEST QUESTIONS**

(These are meant for re-capitulation only. Answers to these questions are not to be submitted for evaluation)

1. Discuss nature and significance and scope of systems audit. Also mentions various steps involved in conducting in information system audit.

2. Discuss system audit of computerised secretarial functions.

3. Write short notes on:
   (a) Norms and procedures for computerisation
   (b) Computer control and security
   (c) Testing of computer system
   (d) Objectives of Information Systems Auditing

4. Discuss the Foundations of Information Systems Auditing.

5. What do you mean by operation control? Describe in details

6. What is the meaning of documentation standards? Explain its importance.

7. State the relationship of Systems audit and various management functions.