7. Information Technology Regulatory Issues

7.1 The IT Act and its Objectives

- The Information Technology Act was enacted on 17th May 2000 primarily to provide legal recognition for electronic transactions and facilitate e-commerce.
- India became the 12th nation in the world to adopt cyber laws by passing the Act.
- The IT Act is based on Model law on e-commerce adopted by UNCITRAL (United Nations Commission on International Trade) of United Nations organization.
- The IT Act extends to whole of India and also applies to any offence or contravention there under committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India.
- The Objectives of the Information Technology Act, 2000 are given as follows:
  - ✦ To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication known as “electronic commerce” ;
  - ✦ To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
  - ✦ To facilitate electronic filing of documents with Government departments;
  - ✦ To facilitate electronic storage of data;
  - ✦ To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
  - ✦ To give legal recognition for keeping of books of accounts by banker’s in electronic form; and
  - ✦ To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.
- Some of the key Issues of electronic information impacting enterprises and auditors are:
  - ✦ **Authenticity:** How do we implement a system that ensures that transactions are genuine and authorized?
  - ✦ **Reliability:** How do we rely on the information, which does not have physical documents?
  - ✦ **Accessibility:** How do we gain access and authenticate this information, which is digital form?

7.2 [Chapter-II] Digital Signature and Electronic Signature

- Chapter II of IT Act gives legal recognition to electronic records and digital signature u/s 3.
- The digital signature is created in two distinct steps.
  - ✦ First, the electronic record is converted into a message digest by using a mathematical function known as “hash function” which digitally freezes the electronic record thus ensuring integrity of content. Any tampering with content of the electronic record will invalidate digital signature.
  - ✦ Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key and which can be verified by anybody who has the public key corresponding to such private key.

7.2.1 [Section 3] Authentication of Electronic Records

1) According to the provisions of Section 3, any subscriber may authenticate an electronic record by affixing his Digital Signature.
2) The authentication of electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform initial electronic record into another electronic record.
3) Any person by the use of a public key of the subscriber can verify the electronic record.
4) The private key and public key are unique to the subscriber and constitute a functioning key pair.

7.2.2 [Section 3A] Electronic Signature

1) Notwithstanding anything contained in section 3, a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which-
   a) is considered reliable; and
   b) may be specified in the Second Schedule.
2) Any electronic signature or electronic authentication technique shall be considered reliable if-
   a) the signature creation data or authentication data are linked to the signatory or authenticator;
   b) the signature creation data or authentication data were under the control of the signatory or the authenticator at the time of signing;
   c) any alteration to the electronic signature made after affixing such signature is detectable;
   d) any alteration to information made after its authentication is detectable; and
   e) it fulfills such other conditions which may be prescribed.
3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is of person by whom it is purported to have been affixed or authenticated.
4) The Central Government may add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature by notification in the Official Gazette.
5) Every notification issued under sub-section (4) shall be laid before each "House of Parliament".

7.3 [Chapter III] Electronic Governance

- Chapter III specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the dispatch and receipt.
- This chapter contains sections 4 to 10.

7.3.1 [Section 4] Legal Recognition of Electronic Records

- Where any law provides that information or any other matter shall be in writing or in typewritten or printed form, then, such requirement shall be deemed to have been satisfied if such information or matter is -
   a) rendered or made available in an electronic form; and
   b) accessible so as to be usable for a subsequent reference.

7.3.2 [Section 5] Legal recognition of Electronic Signatures

- Where any law requires that any information or matter shall be authenticated by affixing the signature of any person, then, such requirement shall be deemed to have been satisfied
  - if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

7.3.3 [Section 6] Use of Electronic Record and Electronic Signature in Government & its agencies

- Section 6 lays down the foundation of Electronic Governance.
- According to the provisions of Section 6,
  - the filing of any form, application or other document, creation, retention or preservation of record
  - issue or grant of any license or permit or
  - receipt or payment in Government offices and its agencies

  may be done through the means of electronic form.
- The appropriate Government office has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection.

7.3.4 [Section 6A] Delivery of services by Service Provider

1) The appropriate Government may authorize by order to any service provider to setup, maintain and upgrade the computerized facilities and perform such other services for efficient delivery of services to the public through electronic means.
2) The appropriate Government may also authorize any service provider authorized to collect, retain and appropriate such service charges from the person availing such services.
3) The appropriate Government may authorize the service providers to collect, retain and appropriate service charges notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification.
4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section.

7.3.5 [Section 7] Retention of Electronic Records

1) 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, if -
   a) the information contained therein remains accessible for a subsequent reference;
   b) the electronic record is retained in the format in which it was originally generated, sent or received or 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.

7.3.6 [Section 7A] Audit of Documents, etc. maintained in Electronic form

- Where in any law, there is a provision for audit of documents, records or information,
  - that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

7.3.7 [Section 8] Publication of rules, regulation, etc., in Electronic Gazette

- Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then,
  - such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:
- The date of publication shall be deemed to be the date of the Gazette which was first published in any form.

7.3.8 [Section 9] Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form

- Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that
  - any Ministry or Department of the Central or State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government
  - should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

7.3.9 [Section 10] Power to make rules by Central Government in respect of Electronic Signature

- The Central Government may, by rules, prescribe
  a) the type of Electronic Signature;
  b) the manner and format in which the Electronic Signature shall be affixed;
  c) the manner or procedure which facilitate identification of person affixing Electronic Signature;
  d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
  e) any other matter which is necessary to give legal effect to Electronic Signature.

7.3.10 [Section 10A] Validity of contracts formed through electronic means

- Where in a contract formation,
  - the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or means,
  - such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

7.4 [Chapter V] Secure Electronic Records and Secure Electronic Signatures

- Chapter V sets out the conditions that would apply to qualify electronic records and digital signatures as being secure. It contains sections 14 to 16.

7.4.1 [Section 14] Secure Electronic Record

- Where any security procedure has been applied to an electronic record at a specific point of time,
  - then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

7.4.2 [Section 15] Secure Electronic Signature

- An electronic signature shall be deemed to be a secure electronic signature if-

i). The signature creation data (means private key of the subscriber), at the time of affixing signature, was under the exclusive control of signatory and no other person; and

ii). The signature creation data was stored and affixed in such exclusive manner as prescribed.

7.4.3 [Section 16] Security Procedures and Practices

- The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices.

7.5 [Chapter IX] Penalties, Compensation and Adjudication

- Chapter IX provides for awarding compensation or damages for certain types of computer frauds.
- It also provides for the appointment of Adjudication Officer for holding an inquiry in relation to certain computer crimes and for awarding compensation.

7.5.1 [Section 43] Penalty and Compensation for damage to computer, computer system, etc.

- 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 network or resource;

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

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

d) damages or causes to be damaged any computer system or network, data, computer data base or any other programme residing in such 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 authorized to access any computer system or computer network by any means;

g) provides any assistance to any person to facilitate access to a 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) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

he shall be liable to pay damages by way of compensation to the person so affected.

7.5.2 [Section 43A] Compensation for failure to protect data

- 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 person so affected.

7.5.3 [Section 44] Penalty for failure to furnish information return, etc.

- If any person who is required under this Act or any rules or regulations made thereunder to -
  a) furnish any document, return or report to the Controller or 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 in the regulation fails to furnish the same, 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.

7.5.4 [Section 45] Residuary Penalty

- 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**.

7.6 [Chapter XI] Offences

- Chapter XI deals with offences under the IT Act.

7.6.1 [Section 65] Tampering with Computer Source Documents

- Whoever knowingly or intentionally conceals, destroys or alters or knowingly causes another to conceal, destroy or alter any computer source code,
  - when the computer source code is required to be maintained by law for the time being in force,
  - shall be punishable **with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both**.

7.6.2 [Section 66] Computer Related Offences

- If any person, dishonestly, or fraudulently, does any act referred to in section 43,
  - he shall be punishable **with imprisonment up to three years or with fine up to five lakh rupees or with both**.

7.6.3 [Section 66A] Punishment for sending offensive messages through communication service.

- Any person who sends, by means of a computer resource or a communication device,-
  a) Any information that is grossly offensive or has menacing character; or
  b) Any information which he knows to be false but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, hatred or ill will; or
  c) any electronic mail or message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

  shall be punishable **with imprisonment for a term up to three years and with fine**.

7.6.4 [Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device

- Whoever dishonestly receives or retains any stolen computer resource or communication device,
  - shall be punished **with imprisonment up to three years or with fine up to rupees one lakh or with both**.

7.6.5 [Section 66C] Punishment for identity theft

- 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 up to three years and with fine up to rupees one lakh**.

7.6.6 [Section 66D] Punishment for cheating by personation by using computer resource

- Whoever, by means of any communication device or computer resource cheats by personating,
  - shall be punished **with imprisonment up to three years and with fine up to one lakh rupees**.

7.6.7 [Section 66E] Punishment for violation of privacy

- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, i.e. violating the privacy of that person,
  - shall be punished **with imprisonment up to three years or with fine not exceeding two lakh rupees, or with both**.

7.6.8 [Section 66F] Punishment for cyber terrorism

- 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 –
     i). denying or cause denial of access to any person authorized to access computer resource; or
     ii). attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
     iii). introducing or causing to introduce any computer contaminant, which causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or 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 authorization or exceeding authorized access, and such conduct obtains
   - access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or
   - any restricted information, data or computer database, which 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.

- Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

7.6.9 [Section 67] Punishment for publishing or transmitting obscene material in electronic form

- 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 tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it,
  - shall be punished on first conviction with imprisonment upto three years and with fine upto five lakh rupees and in the event of a second or subsequent conviction with imprisonment upto five years and also with fine upto ten lakh rupees.

7.6.10 [Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form

- 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 upto five years and with fine upto ten lakh rupees and in the event of second or subsequent conviction with imprisonment upto seven years and also with fine upto ten lakh rupees.

7.6.11 [Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

- 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, 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 upto five years and with a fine upto ten lakh rupees and in the event of second or subsequent conviction with imprisonment of upto seven years and also with fine upto 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 in the interest of science, literature, art or learning or other objects of general concern; or

ii). which is kept or used for bona fide heritage or religious purposes.

7.6.12 [Section 67C] Preservation and Retention of information by intermediaries

1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term upto three years and shall also be liable to fine.

7.6.13 [Section 68] Power of the Controller to give directions

1) The Controller may direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order, if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations.

2) Any person who intentionally or knowingly fails to comply with any order under subsection (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or with both.

7.6.14 [Section 69] Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

1) Where the Central or a State Government or any of its officers specially authorized by the Central or the State Government, if satisfied that it is necessary or expedient so to do,

- in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence,

- for reasons to be recorded in writing, by order, direct any agency of appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency, extend all facilities and technical assistance to -
   a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
   b) intercept, monitor, or decrypt the information, as the case may be; or
   c) provide information stored in computer resource.
4) The subscriber or intermediary or any person who fails to assist such agency shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

7.6.15 [Section 69A] Power to issue directions for blocking for public access of any information through any computer resource

1) Where the Central Government or any of its officers specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do,
   - in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence,
   - for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.
2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.
3) The intermediary who fails to comply with the direction provided shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

7.6.16 [Section 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

1) The Central Government may authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette,.
2) The Intermediary or any person in-charge of the Computer resource shall when called upon by such agency, provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
4) Any intermediary who intentionally or knowingly contravenes the provisions shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

7.6.17 [Section 70] Protected system

1) The appropriate Government may, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure to be a protected system, by notification in the Official Gazette.

   Explanation –

   "Critical Information Infrastructure" means the computer resource, incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems.

3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment for a term upto ten years and shall also be liable to fine.

4) The Central Government shall prescribe the information security practices and procedures for such protected system.

7.6.18 [Section 70A] National nodal agency

1) The Central Government may, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection, by notification published in the official Gazette.

2) The national nodal agency designated shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

3) The manner of performing functions and duties of such agency shall be such as may be prescribed.

7.6.19 [Section 70B] Indian Computer Emergency Response Team to serve as national agency for incident response

1) The Central Government shall, appoint an agency of the government to be called the Indian Computer Emergency Response Team, by notification in the Official Gazette.

2) The Central Government shall provide such agency with a Director-General and such other officers and employees as may be prescribed.

3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

   a) collection, analysis and dissemination of information on cyber incidents;

   b) forecast and alerts of cyber security incidents;

   c) emergency measures for handling cyber security incidents;

   d) coordination of cyber incidents response activities;

   e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

   f) such other functions relating to cyber security as may be prescribed.

5) The manner of performing functions and duties of such agency shall be such as may be prescribed.
6) For carrying out the provisions, such agency may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.
7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction, shall be punishable with imprisonment for a term upto one year or with fine upto one lakh rupees or with both.
8) No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by such agency.

7.6.20 [Section 71] Penalty for misrepresentation

- Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate,
  - shall be punished with imprisonment for a term upto two years, or with fine upto one lakh rupees, or with both.

7.6.21 [Section 72] Penalty for breach of confidentiality and privacy

- Any person who has secured access to any electronic record, book, register, correspondence, information, document or other material
  - without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person
  - shall be punished with imprisonment for a term upto two years, or with fine upto one lakh rupees, or with both.

7.6.22 [Section 72A] Punishment for Disclosure of information in breach of lawful contract

- Any person including an intermediary who 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 upto three years, or with a fine upto five lakh rupees, or with both.

7.6.23 [Section 73] Penalty for publishing Electronic Signature Certificate false in certain particulars

1) No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that -
   a) the Certifying Authority listed in the certificate has not issued it; or
   b) the subscriber listed in the certificate has not accepted it; or
   c) the certificate has been revoked or suspended,

   unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

2) Any person who contravenes the provisions shall be punished with imprisonment for a term upto two years, or with fine upto one lakh rupees, or with both.

7.6.24 [Section 74] Publication for fraudulent purpose

- Whoever knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose
  - shall be punished with imprisonment for a term upto two years, or with fine upto one lakh rupees, or with both.

7.6.25 [Section 75] Act to apply for offences or contraventions committed outside India

1) The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
2) This Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

7.6.26 [Section 76] Confiscation

- Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, shall be liable to confiscation, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened.
- Enterprises need to take steps to ensure compliance with cyber laws. Some key steps for ensuring compliance are given below:
  - Designate a Cyber Law Compliance Officer as required.
  - Conduct regular training of relevant employees on Cyber Law Compliance.
  - Implement strict procedures in HR policy for non-compliance.
  - Implement authentication procedures as suggested in law.
  - Implement policy and procedures for data retention as suggested.
  - Identify and initiate safeguard requirements as applicable under various provisions of the Act such as: Sections 43A, 69, 69A, 69B, etc.
  - Implement applicable standards of data privacy on collection, retention, access, deletion etc.
  - Implement reporting mechanism for compliance with cyber laws.

7.7 [Chapter XII] Intermediaries not to be liable in Certain Cases

- Chapter XII contains section 79.

7.7.1 [Section 79] Exemption from liability of intermediary in certain cases

1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
2) The provisions of sub-section (1) shall apply if-
   a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

b) the intermediary does not -

i). initiate the transmission,

ii). select the receiver of the transmission, and

iii). select or modify the information contained in the transmission

c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

3) The provisions of sub-section (1) shall not apply if -

a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act;

b) upon receiving actual knowledge, or on being notified by appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

7.8 [CHAPTER XIIA] Examiner of Electronic Evidence

7.8.1 [Section 79A] Central Government to notify Examiner of Electronic Evidence

- The Central Government may, for purpose of providing expert opinion on electronic form evidence before any court or other authority specify, any Department, body or agency of the Central or a State Government as an Examiner of Electronic Evidence, by notification in the official Gazette.

7.9 [Chapter XIII] Miscellaneous

- Some miscellaneous sections are as under:

7.9.1 [Section 80] Power of police officer and other officers to enter, search, etc.

1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below rank of a Inspector or any other officer of the Central or a State Government authorized by the Central Government may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

2) Where any person is arrested by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply in relation to any entry, search or arrest, made under this section.

7.9.2 [Section 81] Act to have Overriding effect

- The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.
- PROVIDED that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act, 1970.

7.9.3 [Section 81A] Application of the Act to electronic cheque and truncated cheque

1) The provisions of this Act, shall apply to electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.
2) Every notification made by the Central Government shall be laid, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be.

7.9.4 [Section 84B] Punishment for abetment of offence

- Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

7.9.5 [Section 84C] Punishment for attempt to commit offences

- Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence,
  - shall be punished with imprisonment for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

7.9.6 [Section 85] Offences by Companies

1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

PROVIDED that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

7.10 Requirements of Various Authorities for System Controls & Audit

- Requirements by various statutory bodies' vis-à-vis system and audit requirements have been put including that of IRDA, RBI and SEBI. So, these are just illustrative and not comprehensive.

7.10.1 Requirements of IRDA for System Controls & Audit

- The Insurance Regulatory and Development Authority of India (IRDA) is the apex body overseeing the insurance business in India. It protects the interests of the policyholders, regulates, promotes and ensures orderly growth of the insurance in India.
- Information System Audit aims at providing assurance in respect of Confidentiality, Availability & Integrity for Information system. It also looks at their efficiency, effectiveness & responsiveness.
- **System Audit –**

  These are as follows:

  - ✦ All insurers shall have their systems and process audited at least once in 3 years by a CA firm.
  - ✦ The current internal or concurrent or statutory auditor is not eligible for appointment.
  - ✦ CA firm must be having a minimum of 3-4 years experience of IT systems of banks or mutual funds or insurance companies.
- **Preliminaries –**

  Before proceeding with the audit, the auditor is expected to obtain the following information:

  - ✦ Location(s) from where Investment activity is conducted.
  - ✦ IT Applications used to manage the Insurer's Investment Portfolio.
  - ✦ Obtain the system layout of the IT and network infrastructure including – Server details, database details, type of network connectivity, firewalls other facilities/ utilities.
  - ✦ Are systems and applications hosted at a central location or hosted at different office?
  - ✦ Previous Audit reports and open issues / details of unresolved issues from:
    - Internal Audit,
    - Statutory Audit, and
    - IRDA Inspection / Audit.
  - ✦ Internal circulars and guidelines of the Insurer.
  - ✦ Standard Operating Procedures (SOP).
  - ✦ List of new Products introduced during the period under review along with IRDA approvals.
  - ✦ Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.
  - ✦ IRDA Correspondence files, circulars and notifications issued by IRDA.
  - ✦ IT Security Policy.
  - ✦ Business Continuity Plans.
  - ✦ Network Security Reports pertaining to IT Assets.
- **System Controls –**

  These are as follows:

  - ✦ There should be Electronic transfer of Data without manual intervention. All Systems should be seamlessly integrated. Audit Trail required at every Data entry point. Procedures for reviewing and maintaining audit trail should be implemented.

- ✦ The auditor should comment on the audit trail maintained in the system for various activities.
- ✦ The auditor should review the FOS, MOS and BOS and confirm that the system maintains audit trail for data entry, authorization, cancellation and any subsequent modifications.
- ✦ Further, the auditor shall also ascertain that the system has separate logins for each user and maintains trail of every transaction with respect to login ID, date and time for each data entry, authorization and modifications.

7.10.2 Requirements of RBI for System Controls & Audit

- The Reserve Bank of India (RBI) is India's central banking institution, which formulates the monetary policy with regard to the Indian rupee.
- The Bank was constituted for the need of following:
  - To regulate the issue of banknotes,
  - To maintain reserves with a view to securing monetary stability, and
  - To operate the credit and currency system of the country to its advantage.
- The Reserve Bank of India (RBI) has been at the forefront of recognizing and promoting IS Audit internally and across all the stakeholders including financial institutions. RBI has been proactive in providing guidelines on key areas of IT implementation by using global best practices.
- **System Controls –**

  These are given as follows:
  - ✦ Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming/design.
  - ✦ Contingency plans/procedures in case of failure of system should be introduced/ tested at periodic intervals. EDP auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.
  - ✦ An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements.
  - ✦ In order to bring about uniformity of software used by various branches/offices there should be a formal method of incorporating change in standard software and it should be approved by senior management. Inspection and Audit Department should verify such changes.
  - ✦ Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.
  - ✦ There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.
  - ✦ With a view to provide assurance to banks management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the banks Internal Audit including IS Audit.
- **System Audit –**

  Relevant points are given as follows:

- Banks require a separate IS Audit function within an Internal Audit department led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE). The personnel needs to assume overall responsibility and accountability of IS Audit functions.
- Because the IS Audit is an integral part of the Internal Auditors, auditors will also be required to be independent, competent and exercise due professional care.
- The IS Audit should be independent of the auditee, both in attitude and appearance. The Audit Charter or Policy or engagement letter should address independence & accountability.
- Additionally, to ensure independence for the IS Auditors, Banks should make sure that:
  - Auditors have access to information and applications, and
  - Auditors have the right to conduct independent data inspection and analysis.
- **Competence –**
  - IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience.
  - They should be appropriately qualified, have professional certifications and maintain professional competence through professional education and training.
  - IS Auditors should possess skills that are commensurate with the technology used by a bank. They should be competent audit professionals with relevant experience.
  - Qualifications such as Certified Information Systems Auditor (CISA), Information Systems Audit (ISA), or Certified Information Systems Security Professional (CISSP), along with two or more years of IS Audit experience, are desirable.
- IT Governance, information security governance related aspects, critical IT general controls such as data centre controls and processes and critical business applications/systems having financial/compliance implications, including regulatory reporting, risk management, customer access and MIS systems, needs to be subjected to IS Audit at least once a year.
- IS Audits should also cover branches, with focus on large and medium branches, in areas such as control of passwords, user ids, operating system security, antimalware, maker-checker, segregation of duties, physical security, review of exception reports or audit trails, BCP policy.
- IS Auditors should review the following additional areas that are critical & high risk such as:
  - IT Governance and information security governance structures and practices implemented by the Bank.
  - Testing the controls on new development systems before implementing in live environment.
    - A pre-implementation review of application controls, including security features and controls over change management process, should be performed to confirm that:
    - Controls in existing application are not diluted, while migrating data to new application
    - Controls are designed and implemented to meet requirements of a bank's policies and procedures, apart from regulatory and legal requirements
    - Functionality offered by the application is used to meet appropriate control objectives

- A post implementation review of application controls should be carried out to confirm if the controls as designed are implemented, and are operating, effectively. Periodic review of application controls should be a part of an IS audit scope, in order to detect the impact of application changes on controls.
- Due care should be taken to ensure that IS Auditors have access only to the test environment for performing procedures and data used for testing should be a replica of live environment.
- Detailed audit of SDLC process to confirm that security features are incorporated into a new system, or while modifying an existing system, should be carried out.
- A review of processes followed by an implementation team to ensure data integrity after implementation of a new application or system, and a review of data migration from legacy systems to the new system where applicable should be followed.
- IS Auditors may validate IT risks before launching a product or service. Review by IS Auditor may enable the business teams to incorporate additional controls, if required.
- When IS Auditors believe that bank has accepted a level of residual risk that is inappropriate for the organization, they should discuss the matter with appropriate level of management.

7.10.3 Requirements of SEBI for System Controls & Audit

- The Securities and Exchange Board of India (SEBI) is the regulator for the securities market in India. SEBI has to be responsive to the needs of three groups, which constitute the market:
  - The issuers of securities,
  - The investors, and
  - The market intermediaries.
- Mandatory audits of systems and processes bring transparency in the complex workings of SEBI, prove integrity of the transactions and build confidence among the stakeholders.
- **Systems Audit –**
  - ✦ SEBI had mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.
  - ✦ The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.
  - ✦ Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.
  - ✦ Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit. The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report.
  - ✦ Audit has to be conducted and the Audit report be submitted to the Auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement.

- ✦ The Auditee management provides their comment about the Non-Conformities (NCs) and observations. For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI.
- ✦ The auditor should indicate if a follow-on audit is required to review the status of NCs. The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit.

- **Audit Report Norms –**

  These are given as follows:

  - ✦ The Systems Audit Reports and Compliance Status should be placed before the Governing Board of the Stock Exchanges/Depositories and the system audit report along with comments of Stock Exchanges / Depositories should be communicated to SEBI.
  - ✦ The Audit report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or Observations (or lack of it). For each section, auditors should also provide ways to improve the process, based upon the best practices observed.

- **Auditor Selection Norms –**

  There are various norms for selection of Auditors, which are given as follows:

  - ✦ Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc.
  - ✦ The audit experience should have covered all the Major Areas mentioned under SEBI's Audit Terms of Reference (TOR).
  - ✦ The Auditor shall have relevant industry recognized certification e.g. CISA (Certified Information Systems Auditor), CISM (Certified Information Securities Manager), GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional).
  - ✦ The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.
  - ✦ The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. It should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
  - ✦ The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and unsuitability to perform the audit task.

- **System Controls –**

  These are given as follows:

  - ✦ Further, along with the audit report, Stock Exchanges/Depositories are advised to submit a declaration from the MD/CEO certifying the security and integrity of their IT Systems.
  - ✦ A proper audit trail for upload/modifications/downloads of KYC data to be maintained

7.11 Cyber Forensic and Cyber Fraud Investigation

- Cyber forensics is one of the latest scientific techniques that have emerged due to the effect of increasing computer frauds.

- Cyber means on 'The Net' that is online. Forensics is a scientific method of investigation & analysis techniques to gather, process, interpret, and to use evidence to provide a conclusive description of activities in a way that is suitable for presentation in a court of law. 'Cyber Investigation' is an investigation method gathering digital evidences to be produced in court of law.
- As electronic evidences can be created through use of technology, cyber forensics emphasizes the use of special methods to gather evidences, so that these electronic evidences stand the scrutiny when presented in a court of law.
- To ensure that the objectives are achieved, the experts of the fields use standard processes and globally accept methods so that same result shall always be obtained if the same evidences are checked by another expert, so cyber forensic experts follow standard methods for investigation.
- The IT Act under Section 43A and Section 65 to 67B lists various types of cyber-crimes and specifies penalty for them.

7.12 Security Standards

- Information security is essential in the day-to-day operations of enterprises. Breaches in information security can lead to a substantial impact within the enterprise through. COBIT 5 for Information security published by ISACA, USA highlights the needs for enterprises to ensure required level of security is implemented.
- The ever-increasing need for the enterprise to implement security is highlighted here:
  - ✦ Maintain information risk at an acceptable level and to protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions;
  - ✦ Ensure that services and systems are continuously available to internal and external stakeholders, leading to user satisfaction with IT engagement and services;
  - ✦ Comply with the growing number of relevant laws and regulations as well as contractual requirements and internal policies on information and systems security and protection, and provide transparency on the level of compliance; and
  - ✦ Achieve all of the above while containing the cost of IT services and technology protection.
- **National Cyber Security Policy 2013 –**
  - ✦ Government of India recently published the National Cyber Security Policy 2013 with –
    - **The vision** "To build a secure and resilient cyberspace for citizens, business and Government"
    - **The mission** "To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people processes, technology and cooperation".
  - ✦ The policy document highlights the need for security in the cyberspace and outlines that cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental.
  - ✦ **Major objectives of this policy are given as follows:**
    - To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace;

- To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices;
- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem;
- To enhance and create National and Sectorial level 24*7 mechanisms for obtaining strategic information regarding threats of ICT infrastructure creating scenarios for response, resolution and crisis management;
- To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Center(NCIIPC) and mandating security practices;
- To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, and pilot development of secure ICT products/processes in general and specifically for addressing National Security requirement;
- To improve visibility of the integrity of Information & Communication Technology products & services and establishing infrastructure for testing & validation of security of such product;
- To create a workforce of 500,000 professional skilled in cyber security in the next 5 years through capacity building, skill development and training;
- To provide fiscal benefits to business for adoption of standard security practices & processes;
- To enable protection of information while in process, handling, storage & transit so as to Safeguard privacy of citizen's data and for reducing economic losses due to cybercrime;
- To enable effective prevention, investigation and prosecution of cybercrime and enhancements of law enforcement capabilities through appropriate legislative intervention;
- To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy;
- To develop effective public private partnerships and collaborative engagements through technical and operational and contribution for enhancing the security of cyberspace and
- To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

7.12.1 ISO 27001

- ISO/IEC 27001 (International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC)) defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large.
- This standard is the foundation of Information Security Management. ISO 27001 is for information security – it is a standard written by the world's best experts in the field of information security and aims to provide a methodology for implementation of information security in an organization.
- It enables an organization to get certified, i.e., an independent certification body has confirmed that information security has been implemented in the best possible way in the organization.

- ISO/IEC 27001 formally specifies an Information Security Management System (ISMS).
  - ✦ The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information security risks.
  - ✦ It is a systematic approach to managing confidential or sensitive information so that it remains secure (which means Available, Confidential and with its Integrity intact).
  - ✦ The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts. It encompasses people, processes and IT systems.
- **How the standard works?**
  - ✦ ISO 27001 requires that management:
    - systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
    - designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
    - adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.
- **History**
  - ✦ ISO/IEC 27001 is derived from The British Standard BS 7799 Part 2, published in 1999. BS 7799 Part 2 was revised by BSI in 2002, explicitly incorporating Deming's PDCA process concept, and was adopted by ISO/IEC as ISO/IEC 27001 in 2005. It was extensively revised in 2013, bringing it into line with other ISO certified management systems standards and dropping PDCA concept**.**
- **ISO/IEC 27001:2005**, part of the growing ISO/IEC 27000 family of standards, was an Information Security Management System (ISMS) standard published in October 2005 by ISO/IEC. Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information Security Management Systems – Requirements. It was superseded, in 2013, by ISO/IEC 27001:2013.
  - ✦ **The Plan-Do-Check-Act (PDCA) cycle**
    - ISO 27001 prescribes 'How to manage information security through a system of information security management'.
    - Such a management system consists of four phases that should be continuously implemented in order to minimize risks to the Confidentiality, Integrity and Availability (CIA) of information.
    - The PDCA cyclic process is explained below:
      - i). **The Plan Phase (Establishing the ISMS) –** This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (contains a catalogue of 133 possible controls).
      - ii). **The Do Phase (Implementing and Working of ISMS) –** This phase includes carrying out everything that was planned during the previous phase.

iii). **The Check Phase (Monitoring and Review of the ISMS) –** The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.

iv). **The Act Phase (Update and Improvement of the ISMS) –** The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

- The cycle of these four phases never ends, and all the activities must be implemented cyclically in order to keep ISMS effective. ISO/IEC 27001:2005 applies this to all the process.

- **ISO/IEC 27001:2013** is the first revision of ISO/IEC 27001 that specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System within the context of the organization.
  - ✦ It is an information security standard that was published on 25th September 2013.
  - ✦ It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.
  - ✦ The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
- **Structure**
  - ✦ In the new structure, the Processing Approach, which houses the PDCA model, was eliminated. The reason for this is that the requirement is for continual improvement and PDCA is just one approach to meeting that requirement.
  - ✦ The new standard puts more emphasis on measuring and evaluating how well an organization's ISMS is performing, and there is a new section on outsourcing, which reflects the fact that many organizations rely on third parties to provide some aspects of IT.
  - ✦ Other continuous improvement processes like Six Sigma's DMAIC method can be implemented. More attention is paid to the organizational context of information security, and risk assessment has changed.
  - ✦ Overall, 27001:2013 is designed to fit better alongside other management standards such as ISO 9000 and ISO 20000, and it has more in common with them.
  - ✦ A couple of the major changes to the standard are:
    - Annex A has been revised and restructured; there are now 114 controls under 14 categories rather than the previous 133 controls under 11 categories.
    - The Plan-Do-Check-Act Cycle (PDCA) is no longer mandated.
- **Benefits of ISO 27001**
  - ✦ It can act as the extension of the current quality system to include security.
  - ✦ It provides an opportunity to identify and manage risks to key information and systems assets.
  - ✦ Provides confidence and assurance to trading partners and clients; acts as a marketing tool.
  - ✦ Allows an independent review and assurance to you on information security practices.
- **A company may adopt ISO 27001 for the following reasons**:
  - ✦ It is suitable for protecting critical and sensitive information.

- ✦ It provides a holistic, risk-based approach to secure information and compliance.
- ✦ Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.
- ✦ Demonstrates security status according to internationally accepted criteria.
- ✦ Creates a market differentiation due to prestige, image and external goodwill.
- ✦ If a company is certified once, it is accepted globally.

7.12.2 Standard on Auditing (SA) 402

- Audit Considerations Relating to an Entity using Service Organization, Standard on Auditing (SA) 402 is a revised version of the erstwhile Auditing and Assurance Standard (AAS) 24, "Audit Considerations Relating to Entities Using Service Organizations" issued by the ICAI in 2002.
- The revised Standard deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations.
- SA 402 also deals with the aspects like obtaining an understanding of the services provided by a service organization, including internal control, responding to the assessed risks of material misstatement, Type 1 and Type 2 reports, fraud, non-compliance with laws and regulations and uncorrected misstatements in relation to activities at the service organization and reporting by the user auditor. This SA is effective for audits of financial statements w.e.f. April 1, 2010.

7.12.3 Information Technology Infrastructure Library (ITIL)

- The IT Infrastructure Library (ITIL) is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage.
- ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency.
- It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.
- Although the UK Government originally created the ITIL, it has rapidly been adopted across the world as the standard for best practice in the provision of information technology services.
- ITIL V3 represents an important change in best practice approach, transforming ITIL from providing a good service to being the most innovative and best in class.
- Based on a core of five titles, the changes in ITIL V3 reflect the way IT Service Management has matured over the past decades and change the relationship between IT and business.
  - ✦ **Service Strategy –**
    - This provides guidance on clarification and prioritization of service provider investments in services;
  - ✦ **Service Design –**
    - This provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort;

- **Service Transition –**
  - This relates to the delivery of services required by a business into live/operational use, and often encompasses the "project" side of IT rather than Business As Usual (BAU);
- **Service Operation –**
  - This provides best practice for achieving the delivery of agreed levels of services both to end-users and the customers; and
- **Continual Service Improvement –**
  - This aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes.

7.12.3.1 Details of the ITIL Framework

1) **Service Strategy –**

- The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service provider investments in services.
- It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers.
- The Service Strategy volume provide guidance on the design, development and implementation of service management, not only as an organizational capability, but also as a strategic asset.
- **IT Service Generation –**
  - IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process and Information Technology.
- **Service Portfolio Management –**
  - IT portfolio management is the application of systematic management to investments, projects and activities of enterprise Information Technology (IT) departments.
- **Financial Management –**
  - Financial Management for IT Services' aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.
- **Demand Management –**
  - Demand management is a planning methodology used to manage and forecast the demand of products and services.
- **Business Relationship Management –**
  - Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services via networks.

2) **Service Design –**

- Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations.

- It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings.
- The Service Design volume provides guidance on the design and development of services and service management processes. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.
- **Service Catalogue Management –**
  - ✦ Service Catalogue management maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers.
- **Service Level Management –**
  - ✦ Service-level management provides for continual identification, monitoring and review of the levels of IT services specified in the Service-Level Agreements (SLAs).
- **Availability Management –**
  - ✦ Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost.
- **Capacity Management –**
  - ✦ Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands.
- **IT Service Continuity Management –**
  - ✦ IT Service Continuity Management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs.
- **Information Security Management –**
  - ✦ A basic goal of security management is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization.
- **Supplier Management –**
  - ✦ The purpose of Supplier Management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements.

3) Service Transition –

- Service Transition planning provides guidance on managing the complexity of changes to services and service management processes to prevent undesired consequences whilst permitting for innovation.
- It provides guidance on the support mechanism on transferring the control of services between customers and service providers.
- The Service Transition volume provides guidance on the development and improvement of capabilities for transitioning new and changed services into operations.

- **Service Transition Planning and Support –**
  - ✦ The service transition planning and support process ensures the orderly transition of a new or modified service into production, together with the necessary adaptations to the service management processes.
- **Change management and Evaluation –**
  - ✦ This aims to ensure that standardized methods and procedures are used for efficient handling of all changes.
- **Service Asset and Configuration Management –**
  - ✦ Service Asset and Configuration Management primarily focused on maintaining information about Configuration Items required to deliver an IT service, including their relationships.
- **Release and Deployment Management –**
  - ✦ Release and deployment management is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure.
- **Service Validation and Testing –**
  - ✦ The objective of ITIL Service Validation and Testing is to ensure that deployed Releases and the resulting services meet customer expectations, and to verify that IT operations are able to support the new service.
- **Knowledge Management –**
  - ✦ Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organisational knowledge.

4) Service Operation –

- Service Operation provides guidance on the management of a service through its day-to-day production life.
- It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.
- **Functions**: The major functions are as follows:
  - ✦ **Service Desk –**
    - The service desk is primarily associated with the Service Operation lifecycle stage. Tasks include handling incidents & requests and providing an interface for other ITSM process.
  - ✦ **Application management –**
    - ITIL application management encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects.
  - ✦ **IT Operations –**
    - IT Operations primarily work from documented processes & procedures and should be concerned with a number of specific sub-processes, such as: output management, job scheduling, backup & restore, network management, system & database management.

- ✦ **IT Technical Support –**
  - IT technical support provides a number of specialist functions: research and evaluation, market intelligence, proof of concept & pilot engineering, specialist technical expertise.

- **Incident Management –**
  - ✦ Incident management aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.
- **Request fulfillment –**
  - ✦ Request fulfillment (or request management) focuses on fulfilling Service Requests, which are often minor changes (e.g., requests to change a password) or requests for information.
- **Event Management –**
  - ✦ An event may indicate that something is not functioning correctly, leading to an incident being logged. Event management generates and detects notifications, while monitoring checks the status of components even when no events are occurring.

5) Continual Service Improvement –

- Continual Service Improvement provides guidance on the measurement of service performance through the service life-cycle, suggesting improvements to ensure that a service delivers the maximum benefit.
- This volume provides guidance on creating and maintaining value for customers through improved design, introduction, and operation of services.
- It combines principles, practices and methods from change management, quality management, and capability improvement to achieve incremental and significant improvements in service quality, operational efficiency, and business continuity.
- It provides guidance on linking improvement efforts and outcomes with service strategy, design, and transition, focusing on increasing the efficiency, maximizing the effectiveness and optimizing the cost of services and the underlying IT Service Management processes.

7.13 Key Definitions

(1) In this Act, unless the context otherwise requires,

(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;

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

(c) "**Adjudicating Officer**" means adjudicating officer appointed under subsection (1) of section 46;

(d) "**Affixing Electronic 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 Electronic Signature;

(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;

(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;

(g) "**Certifying Authority**" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24;

(h) "**Certification Practice Statement**" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;

(ha) "**Communication Device**" means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image.

(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;

(j) "**Computer Network**" means the interconnection of one or more Computers or Computer systems or Communication device through-

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

(k) "**Computer Resource**" means computer, communication device, computer system, computer network, data, computer database or software;

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

(m) "**Controller**" means the Controller of Certifying Authorities appointed under section 17(7);

(n) "**Cyber Appellate Tribunal**" means the Cyber Appellate Tribunal established under section 48(1).

(na) "**Cyber Cafe**" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

(nb) "**Cyber Security**" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

(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 or stored internally in the memory of the computer;

(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;

(q) "**Digital Signature Certificate**" means a Digital Signature Certificate issued under section 35(4);

(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;

(s) "**Electronic Gazette**" means official Gazette published in the electronic form;

(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;

(ta) "**electronic signature**" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature

(tb) "**Electronic Signature Certificate**" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"

(u) "**Function**", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(ua) "**Indian Computer Emergency Response Team**" means an agency established u/s 70 B (1).

(v) "**Information**" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

(w) "**Intermediary**" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes;

(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 private key;

(y) "**Law**" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(z) "**License**" means a license granted to a Certifying Authority under section 24;

(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;

(zb) “**Prescribed**" means prescribed by rules made under this Act;

(zc) “**Private Key**" means the key of a key pair used to create a digital signature;

(zd) “**Public Key**" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(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;

(zf) "**Security Procedure**" means the security procedure prescribed u/s 16 by the Central Government;

(zg) "**Subscriber**" means a person in whose name the Electronic Signature Certificate is issued;

(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.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

Explanation –

For the purposes of this section, -

(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 ;

(ii) "**computer database**" 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 formalized 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 re-arrange 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.