CHAPTER-7
INFORMATION TECHNOLOGY REGULATORY ISSUES

7.1. The Objectives of the Act are given as follows:

1) To grant legal recognition **E-Commerce**
2) To give legal recognition to **Digital signatures**
3) To facilitate **E-Filing** of documents with Government departments;
4) To facilitate **electronic storage** of data;
5) To facilitate and give legal sanction to electronic **fund transfers** between banks and financial institutions;
6) To give legal recognition for **keeping of books** of accounts by banker's in electronic form; and
7) 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.

The IT Act extends to whole of India and also applies to any offence or contravention there under committed outside India by any person {section 1 (2)} read with Section 75. The Act applies to offence or contravention committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India.

7.2. Digital Signature and Electronic Signature

Section 3 gives legal recognition to electronic records and digital signatures. The section provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. 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 the integrity of the content of the intended communication contained in the electronic record. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature.

7.3. Section 3 Authentication of Electronic Records:

1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.
2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the 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 the public key are unique to the subscriber and constitute a functioning key pair.

7.4. Section 3A Electronic Signature

1) Notwithstanding anything contained in section 3, but subject to the provisions of sub- section (2) 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) For the purposes of this section 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 of 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 fulfills such other conditions which may be prescribed.

7.5. Section 4 provides for legal recognition of electronic records

It provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form.

7.6. Section 5 provides for legal recognition of Digital Signatures

Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the Central Government.

7.7. Section 6 lays down the foundation of Electronic Governance

It provides that the filing of any form, application or other documents, creation, retention or preservation of records, 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.

7.8. Section 7 Retention of Electronic Records

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, -

1) the information contained therein remains accessible so as to be usable for a subsequent reference;
2) 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;
3) 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:

However, 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

7.9. Section 7A Audit of Documents etc. in Electronic form

Where in any law for the time being in force, 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

7.10. Section 8 provides for the publication of rules, regulations and notifications in the Electronic Gazette

It provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form. It also provides where the Official Gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

7.11. 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:

7.12. 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 Government or the 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.

7.13. Section 10 Power to make rules by Central Government in respect of Electronic Signature

The Central Government may, for the purposes of this Act, by rules, prescribe

1) the type of Electronic Signature;
2) the manner and format in which the Electronic Signature shall be affixed;
3) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;
4) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
5) any other matter which is necessary to give legal effect to Electronic Signature.

7.14. 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 by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

7.15. Section 15 Secure Electronic Signature

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

1) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
2) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

7.16. Section 16 provides for the power of the Central Government

To prescribe the security procedure in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability and cost of alternative procedures, volume of similar transactions entered into by other parties etc.

7.17. 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 –

1) accesses or secures access to such computer, computer system or computer network or computer resource.
2) 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;
3) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4) 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;
5) disrupts or causes disruption of any computer, computer system or computer network;
6) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means; 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,
7) 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.
8) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.
9) 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.

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 the person so affected.

7.18. 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 there under to - (a) furnish any document, return or report to the Controller or the Certifying Authority, fails to

1) furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
2) 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:
3) 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.

7.19. Section 45 provides for 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.

7.20. Section 65 Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or 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 2 lakh rupees, or with both.

7.21. 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 for a term which may extend to three years or with fine which may extend to 5 lakh rupees or with both

7.22. Section 66A Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

1) Any information that is grossly offensive or has menacing character; or
2) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device;
3) any electronic mail or electronic mail 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 which may extend to two three years and with fine.

7.23. Section 66B Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives 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.

7.24. 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 of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

7.25. Section 66D Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, 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 rupees.

7.26. 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, 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

7.27. Section 66F Punishment for cyber terrorism: whoever,-

1) 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 –
   - **a)** Denying or cause the denial of access to any person authorized to access computer resource; or
   - **b)** Attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or
   - **c)** 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

2) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of 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, 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, r 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'.

7.28. 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 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 a 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.

7.29. 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 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.

7.30. Section 67B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form: Whoever,-

1) 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
2) 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
3) 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
4) Facilitates abusing children online; or
5) 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 a 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:

7.31. 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 which may extend to three years and shall also be liable to fine.

7.32. Section 68 Power of Controller to give directions

1) The Controller may, by order, 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 made there under.
2) Any person who intentionally or knowingly fails to comply with any order under sub-section (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.

7.33. Section 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

1) Where the central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, 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 relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the 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 which has been directed under sub section (1), 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;
   c) provide information stored in computer resource.
4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

7.34. 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 officer specially authorised 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 relating to above, it may subject to the provisions of sub-sections (2), 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 issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine

7.35. 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, 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, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorised under sub-section (1), 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 of sub- section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

7.36. Section 70 Protected system

1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).
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 of either description for a term which may extend to 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.

7.37. Section 70A National nodal agency

1) The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.
2) The national nodal agency designated under sub-section (1) 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 the agency referred to in sub-section shall be such as may be prescribed.

7.38. Section 70B Indian Computer Emergency Response Team to serve as national agency for incident response

1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.
2) The Central Government shall provide the agency referred to in sub-section (1) 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
   b) emergency measures for handling cyber security incidents;
   c) coordination of cyber incidents response activities;
   d) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
   e) such other functions relating to cyber security as may be prescribed.
5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.
6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) 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 under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to 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 authorised in this behalf by the agency referred to in sub-section (1)

7.39. 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, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

7.40. Section 72 Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations madethere under, 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 which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

7.41. Section 72A Punishment for Disclosure of information in breach of lawful contract

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.

7.42. 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 of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

7.43. 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 which may extend to two years, or with fine which may extend to one lakh rupees, or with both

7.44. Section 75 Act to apply for offence or contraventions committed outside India

1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

2) For the purposes of sub-section (1), 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.

7.45. Section 76 Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation

However,

where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit. Enterprises need to take steps to ensure compliance with cyber laws. Some key steps for ensuring compliance are given below:

1) Designate a Cyber Law Compliance Officer as required.
2) Conduct regular training of relevant employees on Cyber Law Compliance.
3) Implement strict procedures in HR policy for non-compliance.
4) Implement authentication procedures as suggested in law.
5) Implement policy and procedures for data retention as suggested.
6) Identify and initiate safeguard requirements as applicable under various provisions of the Act such as: Sections 43A, 69, 69A, 69B, etc.
7) Implement applicable standards of data privacy on collection, retention, access, deletion etc.
8) Implement reporting mechanism for compliance with cyber laws.

7.46. Intermediaries not to be liable in Certain Cases Chapter XII

Chapter XII contains section 79 which provides that the Network Service Providers shall be liable for any third party information or data made available by him if he proves that the offence was committed without his knowledge or consent.

7.47. 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 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 the 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 the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

7.48. Section 79A Central Government to notify Examiner of Electronic Evidence

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

7.49. Section 81A Application of the Act to Electronic cheque and Truncated cheque

1) The provisions of this Act, for the time being in force, shall apply to, or in relation 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 (26 of 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 under subsection (1) shall be laid, as soon as may be after it is made, 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; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under the notification.

7.50. Section 84 C 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, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, 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.

7.51. 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 there under 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:
However, 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.

7.52. 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 has a significant role to play in the emerging Insurance Sector. Information System Audit aims at providing assurance in respect of Confidentiality, Availability and Integrity for Information systems. It also looks at their efficiency, effectiveness and responsiveness. It focuses on compliance with laws and regulations, which are given as follows:

1) System Audit: These are as follows:

a) All insurers shall have their systems and process audited at least once in three years by a CA firm.

b) In doing so, the current internal or concurrent or statutory auditor is not eligible for appointment.

c) CA firm must be having a minimum of 3-4 years experience of IT systems of banks or mutual funds or insurance companies.

2) Preliminaries

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

a) Location(s) from where Investment activity is conducted.

b) IT Applications used to manage the Insurer's Investment Portfolio.

c) Obtain the system layout of the IT and network infrastructure including: Server details, database details, type of network connectivity, firewalls other facilities/ utilities (describe).

d) Previous Audit reports and open issues / details of unresolved issues from:
i) Internal Audit,
ii) Statutory Audit, and
iii) IRDA Inspection / Audit.

e) Internal circulars and guidelines of the Insurer.

f) Standard Operating Procedures (SOP).

g) List of new Products/funds introduced during the period under review along with IRDA approvals for the same.

h) Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.

i) IRDA Correspondence files, circulars and notifications issued by IRDA.

j) IT Security Policy.

k) Business Continuity Plans.

l) Network Security Reports pertaining to IT Assets.

3) **System Controls:** These are as follows:

a) 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.

b) 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.

c) 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.

7.53. Requirements of RBI for System Controls & Audit

Primarily, RBI suggests that senior management and regulators need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the IT related risks are managed. Sample areas of review covered by IS Audit assignments are given here.

1) **System Controls:** These are given as follows:

a) 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. System person would only make modifications/improvements to programs and the operating persons would only use such programs without having the right to make any modifications.

b) 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.

c) An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements.

d) 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 from the view-point of control and for its implementation in other branches in order to maintain uniformity.

e) Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.

f) There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.

g) With a view to provide assurance to bank's 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 to validate the approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Charter/Audit Policy.

2) **System Audit:** Relevant points are given as follows:

a) In this regard, 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. Where the bank leverages external resources for conducting IS Audit on areas where skills are lacking, the responsibility and accountability for such external IS Audits still remain with the IS Audit Head and CAE.

b) 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.

c) 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. As IT encompasses a wide range of technologies, IS Auditors should possess skills that are commensurate with the technology used by a bank. They should be competent audit professionals with sufficient and relevant experience. Qualifications such as CISA (offered by ISACA), DISA (offered by ICAI), or CISSP (offered by ISC2), along with two or more years of IS Audit experience, are desirable. Similar qualification criteria should also be insisted upon, in case of outsourced professional service providers.

d) IT governance, information security governance related aspects, critical IT general controls such as data center controls and processes and critical business applications/systems having financial/compliance implications, including regulatory reporting, risk management, customer access (delivery channels) and MIS systems, needs to be subjected to IS Audit at least once a year (or more frequently, if warranted by the risk assessment).

e) 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, anti- malware, maker-checker, segregation of duties, physical security, review of exception reports or audit trails, BCP policy and or testing.

f) IS Auditors should review the following additional areas that are critical and high risk such as:

i) IT Governance and information security governance structures and practices implemented by the Bank.

ii) Testing the controls on new development systems before implementing them in live environment.

iii) A post implementation review of application controls should be carried out to confirm if the controls as designed are implemented, and are operating, effectively. Due care should be taken to ensure that IS Auditors have access only to the test environment for performing the procedures and data used for testing should be, as far as practical, be a replica of live environment.

iv) 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.

v) 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.

vi) IS Auditors may validate IT risks (identified by business teams) before launching a product or service. Review by IS Auditor may enable the business teams to incorporate additional controls, if required, in the system before the launch.

g) IT governance, information security governance related aspects , critical IT general controls like data centre controls and processes and critical business applications having financial/ compliance/ customer access(like delivery channels) including MIS and regulatory reporting systems need to be audited at least once a year (or more frequently, if warranted by the risk assessment).
In addition, RBI has an inspection wing, which does inspection of banking and non-banking financial institutions.

7.54. Requirements of SEBI for System Controls & Audit

1) **Systems Audit:** SEBI had mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.
   a) The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.

   b) 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.

   c) Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.

   d) 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

   e) 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 report should also take previous audit reports in consideration and cover any open items therein.

   f) 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. Sample areas of review covered by IS Audit assignments are given here.

2) **Audit Report Norms:** These are given as follows:
   a) 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

   b) 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 qualitative input about ways to improve the process, based upon the best practices observed.

3) **Auditor Selection Norms:** There are various norms for selection of Auditors, which are given as follows:
   a) 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).

   b) The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as $(ISC)^2$.

   c) The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.

   d) 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.

   e) The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

4) **System Controls:** These are given as follows:
   a) 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.

   b) A proper audit trail for upload/modifications/downloads of KYC data to be maintained

   Department of Electronics & IT, Ministry of Communication and IT, Government of India, maintains a panel of systems auditors, which are used by government enterprises for getting system audit done. This provides information on scope of different types of systems audit which is used as reference by auditee firms for getting systems audit done.

7.55. Cyber Forensic and Cyber Fraud Investigation

Cyber, means on 'The Net' that is online. Forensics is a scientific method of investigation and 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. Considering 'Cyber' and 'Investigation' together will lead us to conclude that 'Cyber Investigation' is an investigation method gathering digital evidences to be produced in court of law.

Court rulings and amendments to cyber laws now permit courts to rely upon digital evidences. 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 rigours/scrutiny when presented in a court of law.
To ensure that the above 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, that is why cyber forensic experts follow standard methods for investigation

7.56. 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, for example, financial or operational damages. In addition, the enterprise can be exposed to external impacts such as reputational or legal risk, which can jeopardize customer or employee relations or even endanger the survival of the enterprise. 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:

1) Maintain information risk at an acceptable level and to protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions;
2) Ensure that services and systems are continuously available to internal and external stakeholders, leading to user satisfaction with IT engagement and services;
3) 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
4) Achieve all of the above while containing the cost of IT services and technology protection.

Considering the importance of security, 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" and 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".

Major objectives of this policy are given as follows:

1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of T all sectors of the economy;

2) 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 by way of conformity assessment (product, process, technology, & people);

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem;

4) 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 through effective predicative, protective, response and recovery actions;

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24*7 National Critical Information Infrastructure Protection Center(NCIIPC) and mandating security practices related to the design, acquisition, development and operation of information resources;

6) 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 requirements;

7) To improve visibility of the integrity of ICT products & services and establishing infrastructure for testing & validation of security of such products;
   a) To create a workforce of 500,000 professional skilled in cyber security in the next 5 years through capacity building, skill development and training;

   b) To provide fiscal benefits to businesses for adoption of standard security practices and processes;

c) 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 or data theft;

d) To enable effective prevention, investigation and prosecution of cybercrime and enhancements of law enforcement capabilities through appropriate legislative intervention;

e) To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy;

f) To develop effective public private partnerships and collaborative engagements through technical and operational and contribution for enhancing the security of cyberspace and

g) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Based on the key aspects of National Cyber Security Policy 2013, we can understand that Chartered Accountants in their role as accountants and auditors have another important role to play in ensuring compliance of security and also pro-actively provide assurance on the state of IT security in an enterprise.

7.57. ISO 27001

ISO 27001 is the international best practice and standard for an Information Security Management System (ISMS). An ISMS is a systematic approach to managing confidential or sensitive information so that it remains secure (which means available, confidential and with its integrity intact).

ISO 27001 defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large. It is safe to say that this standard is the foundation of information security management. ISO 27001 is for information security; the same thing that ISO 9001 is for quality

ISO/IEC 27001:2005, usually referred to just as ISO 27001, is the best practice specification that helps businesses and organizations throughout the world to develop a best-in-class ISMS. The Standard was published jointly by the International Security Office (ISO) and the International Electro-technical Commission (IEC). The British standard BS7799-2 was the forerunner for ISO 27001.

1) **Four phases of ISMS:** ISO 27001 prescribes 'how to manage information security through a system of information security management'. Such a management system, just like ISO 9001 or ISO 14001, consists of four phases that should be continuously implemented in order to minimize risks to the CIA of information.
   - **a)** These phases are given as follows:
   - **b)** **The Plan Phase –** This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
   - **c)** **The Do Phase –** This phase includes carrying out everything that was planned during the previous phase.
   - **d)** **The Check Phase –** 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.
   - **e)** **The Act Phase –** 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 the ISMS effective. The detail description of all these aforementioned phases is given as follows:

2) **The Plan phase:** The Plan phase consists of the following steps
   - **a)** Determining the scope of the ISMS;
   - **b)** Writing an ISMS Policy;
   - **c)** Identifying the methodology for risk assessment and determining the criteria for risk acceptance;

d) Identification of assets, vulnerabilities and threats;
e) Evaluating the size of risks;
f) Identification and assessment of risk treatment options;
g) Selection of controls for risk treatment;
h) Obtaining management approval for residual risks;
i) Obtaining management approval for implementation of the ISMS; and
j) Writing a Statement of applicability that lists all applicable controls, states which of them have already been implemented, and those which are not applicable.

3) The Do phase: This phase consists of the following activities:
a) Writing a risk treatment plan – describes who, how, when and with what budget applicable controls should be implemented;
b) Implementing the risk treatment plan;
c) Implementing applicable security controls;
d) Determining how to measure the effectiveness of controls;
e) Carrying out awareness programs and training of employees;
f) Management of the normal operation of the ISMS;
g) Management of ISMS resources; and
h) Implementation of procedures for detecting and managing security incidents.

4) The Check phase: This phase includes the following:
a) Implementation of procedures and other controls for monitoring and reviewing in order to establish any violation, incorrect data processing, whether the security activities are carried out as expected, etc.;
b) Regular reviews of the effectiveness of the ISMS;
c) Measuring the effectiveness of controls;
d) Reviewing risk assessment at regular intervals;
e) Internal audits at planned intervals;
f) Management reviews to ensure that the ISMS is functioning and to identify opportunities for improvement;
g) Updating security plans in order to take account of other monitoring and reviewing activities; and
h) Keeping records of activities and incidents that may affect the effectiveness of the ISMS.

5) The Act phase: This phase includes the following:
a) Implementation of identified improvements in the ISMS;
b) Taking corrective and preventive action; applying own and others' security experiences;
c) Communicating activities and improvements to all stakeholders; and
d) Ensuring that improvements achieve the desired objectives.

6) Other Related Aspects: ISO 27001 requires that management:
a) Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
b) Design and implement 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
c) Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

7) The key benefits of ISO 27001 are given as follows:
a) It can act as the extension of the current quality system to include security.
b) It provides an opportunity to identify and manage risks to key information and systems assets.
c) Provides confidence and assurance to trading partners and clients; acts as a marketing tool.
d) Allows an independent review and assurance to you on information security practices.

8) A company may adopt ISO 27001 for the following reasons:

a) It is suitable for protecting critical and sensitive information.
b) It provides a holistic, risk-based approach to secure information and compliance.
c) Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.
d) Demonstrates security status according to internationally accepted criteria.
e) Creates a market differentiation due to prestige, image and external goodwill.
f) If a company is certified once, it is accepted globally.

As per recent statistical data, there are more than 500 Indian Companies, which have acquired the ISO 27001 certificate and this data is increasing on a regular basis.

7.58. ITIL (IT Infrastructure Library)

The Information Technology 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.

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. At the same time the interface between old and new approaches is seamless, making adoption simple for those experienced in ITIL V2. ITIL V3 makes the link between ITIL's best practice and business benefits both clearer and stronger. 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. Whereas previously ITIL worked to align Service Management with business strategy, ITIL V3 integrates into a single lifecycle.

This release of ITIL brought with it an important change of emphasis, from an operationally focused set of processes to a mature service management set of practice guidance. It also brought a rationalization in the number of volumes included in the set, which now comprises the following:

1) Service Strategy,
2) Service Design,
3) Service Transition,
4) Service Operation, and
5) Continual Service Improvement.

Details of the ITIL Framework: Details of these aforementioned volumes are given as follows:

1) **Service Strategy:** Service Strategy deals with the strategic management approach in respect of IT Service Management; strategic analysis, planning, positioning, and implementation relating to service models, strategies, and strategic objectives. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers.

   The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset. It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle. Service Strategy decisions have far- reaching consequences including those related to delayed effect
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.
3) **Service Transition:** Service Transition provides guidance on the service design and implementation, ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively

The Service Transition volume provides guidance on the development and improvement of capabilities for transitioning new and changed services into operations. Guidance is provided on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation, whilst controlling the risks of failure and disruption. It combines the processes in Release, Program and Risk Management and sets them in the practical context of Service Management.

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.

   This volume presents practices in the management of service operations and includes guidance on achieving efficiency and effectiveness in the delivery and support of services to ensure value for the customer and the service provider. Service operations ultimately fulfill the strategic objectives, which make it a critical capability. Guidance is provided on techniques to maintain service operations stability whilst allowing for changes in design, scope, scale, and service levels.

   Service Operation provides detailed guidelines on processes, methods, and tools in addressing the proactive and reactive control perspectives. Managers and practitioners are provided with knowledge; enabling them to make better informed decisions in areas

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