

Chapter – 7

Information Technology Regulatory Issues

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. When the Information Technology Act, 2000 was introduced, it was the first information technology legislation introduced in India. 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 was amended by passing of the Information Technology (Amendment) Act 2008 (Effective from October 27, 2009). The amended Act casts responsibility on body corporate to protect sensitive personal information (Sec. 43A). It recognizes and punishes offences by companies and individual (employee) actions (Sec. 43, 66 to 66F, 67..) such as sending offensive messages using electronic medium or using body corporate's IT for unacceptable purposes, stealing computer resources, unauthorized access to computer resources, identity theft/cheating by personating using computer, violation of privacy, cyber terrorism, offences using computer and publishing or transmitting obscene material.

The following rules have been issued for IT Act 2008:

1. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
2. Information Technology (Electronic Service Delivery) Rules, 2011.
3. Information Technology (Intermediaries guidelines) Rule , 2011

The Objectives of the Act are given as follows:

- 1) To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
- 2) To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
- 3) To facilitate electronic 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;

Some of the key Issues of electronic information impacting enterprises and auditors are:

1. **Authenticity:** How do we implement a system that ensures that transactions are genuine and authorized?
2. **Reliability:** How do we rely on the information, which does not have physical documents?
3. **Accessibility:** How do we gain access and authenticate this information, which is digital form?

A good understanding of the provisions of IT Act will provide answer to these issues.

Key Definitions

As enterprises increasingly use digital signature technologies to support e-commerce, legal issues such as non-repudiation, online contracts and protection of intellectual property have become more common. The IT Act provides various definitions of different technological terms; some of the key definitions are given below:

1. **"Access"** with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
2. **"Addressee"** means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
3. **"Adjudicating Officer"** means adjudicating officer appointed under subsection (1) of section 46;
4. **"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;
5. **"Appropriate Government"** means as respects any matter.
 - enumerated in List II of the Seventh Schedule to the Constitution;
 - 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;
6. **"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;
7. **"Certifying Authority"** means a person who has been granted a license to issue a Electronic Signature Certificate under section 24;
8. **"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;
9. **"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.
10. **"Computer"** means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
11. **"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;
12. **"Computer Resource"** means computer, communication device, computer system, computer network, data, computer database or software;
13. **"Computer System"** means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data,

that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

14. **"Controller"** means the Controller of Certifying Authorities appointed under sub-section (7) of section 17;
15. **"Cyber Appellate Tribunal"** means the Cyber Appellate * Tribunal established under sub-section (1) of section 48.
 - A. **"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.
 - B. **"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.
16. **"Data"** means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
17. **"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;
18. **"Digital Signature Certificate"** means a Digital Signature Certificate issued under sub-section (4) of section 35;
19. **"Electronic Form"** with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
20. **"Electronic Gazette"** means official Gazette published in the electronic form;
21. **"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;
 - A. **"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
 - B. **"Electronic Signature Certificate"** means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"
22. **"Function"**, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
23. **"Information"** includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;
24. **"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;
25. **"Key Pair"**, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

26. **"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;
27. **"License"** means a license granted to a Certifying Authority under section 24;
- A. **"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;
 - B. **"Prescribed"** means prescribed by rules made under this Act;
 - C. **"Private Key"** means the key of a key pair used to create a digital signature;
 - D. **"Public Key"** means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;
 - E. **"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;
 - F. **"Security Procedure"** means the security procedure prescribed under section 16 by the Central Government;
 - G. **"Subscriber"** means a person in whose name the Electronic Signature Certificate is issued;
 - H. **"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.

[Chapter-II] Digital Signature and Electronic Signature

This chapter of IT Act gives legal recognition to electronic records and digital signatures. It contains only **Section 3**. 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.

1. 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. Any tampering with the contents of the electronic record will immediately invalidate the digital signature.
2. 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.

[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.

[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;
 - (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 that of the person by whom it is purported to have been affixed or authenticated.
- (4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule;
- ⁶⁾ PROVIDED that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.
- ⁷⁾ (5) Every notification issued under sub-section (4) shall be laid before each "House of Parliament".

[Chapter III] Electronic Governance

This chapter is one of the most important chapters. It 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.

[Section 4] Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

- (a) rendered or made available in an electronic form; and
- (b) accessible so as to be usable for a subsequent reference.

[Section 5] Legal recognition of Electronic Signatures

Where any law requires that any information or matter shall be authenticated by affixing the signature or any

document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, 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.

[Section 6] Use of Electronic Records and Electronic Signatures in Government and its agencies

1. Where any law provides for -

- (a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
- (b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
- (c) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

2. The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe-

- a. the manner and format in which such electronic records shall be filed, created or issued;
- b. the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

[Section 6A] Delivery of services by Service Provider

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to setup, maintain and upgrade the computerized facilities and perform such other services as it may specify by notification in the Official Gazette.

[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 so as to be usable for a subsequent reference;
- (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
- (c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

[Section 7A] Audit of Documents, etc. maintained 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.

[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:

PROVIDED that where any rule, regulation, order, bye-law, notification or any other matters 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.

[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.

[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 (a)

- 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 facilitates identification of the person affixing the 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.

[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.

[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.**

[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.

[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.

[Section 16] Security Procedures and Practices

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

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

[Chapter IX] Penalties, Compensation and Adjudication

Chapter IX contains sections 43 to 47. It 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. Sections 43 to 45 deal with different nature of penalties.

[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 computer network or computer resource;
- b. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- c. 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;
- d. disrupts or causes disruption of any computer, computer system or computer network;
- e. denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
- f. 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;
- g. 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;
- h. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
- i. 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.

[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 the person so affected.

[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 furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
- B. file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
- C. maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

[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.

[Chapter XI] Offences

Apart from giving recognition to electronic contracts, the IT Act identifies certain acts as "Computer Crimes" and provides penalties for these offences. It is necessary for every user to Internet and other proprietary networks to avoid inadvertently committing any action, which can be termed as a "Computer Crime". The Act lists common crimes that can be perpetuated in the electronic society and specifies penalty. The Computer crimes that are recognized by the Act could affect:

1. Hackers
2. Digital Contract parties
3. The Digital IC users
4. Netizen
5. Web Site owners/Content
6. creators Software
7. professionals
8. Auditor
9. Certifying authorities web hosting firms

Chapter XI deals with offences under the IT Act. Auditors need to have good understanding of various provisions of this section so as to review compliance as required.

[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 programme, 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 two lakh rupees, or with both.

[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 five lakh rupees or with both.

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

- A. Any person who sends, by means of a computer resource or a communication device,-
- B. Any information that is grossly offensive or has menacing character; or
- C. 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; or
- D. 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 three years and with fine.

[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.

[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.

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

Whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

[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 punishable with imprisonment which may be extended upto three years or with fine not exceeding two lakh or with both.

[Section 66F] Punishment for cyber terrorism

- (1) 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 the 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,

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

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization 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, 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.

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

[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.

[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.

[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, 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

facilitates abusing children online; or

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:

Provide 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 -

1. 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
2. which is kept or used for bona fide heritage or religious purposes.

[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

[Section 68] Power of the 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 thereunder.

(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.

[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 officers specially authorized 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.

(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; or (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.

[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 relating to above, it may subject to the provisions of sub-section (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 shall also be liable to fine.

[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, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
2. The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
3. 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.

[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, authorize the persons who are authorized 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.

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

[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 (1) shall be such as may be prescribed.

[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;
- (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 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 authorized in this behalf by the agency referred to in sub-section (1).

[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.

[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 made thereunder, 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.

[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.

[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.

[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.

[Section 75] Act to apply for offences 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.

[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:

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.

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

Chapter XII contains section 79.

[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 hosted; 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.

[CHAPTER XIIA] Examiner of Electronic Evidence

[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.

[Chapter XIII] Miscellaneous

Some miscellaneous sections are as under:

[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 the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf 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 under sub-section (1) 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 (2 of 1974) shall, subject to the

provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

[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.

[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.

[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.

[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, 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.

[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.

Requirements of Various Authorities for System Controls & Audit

Under this part, requirements by various statutory bodies' vis-à-vis system and audit requirements have been put including that of IRDA, RBI and SEBI. It is important to note that these are just illustrative and not comprehensive.

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:

(i) System Audit: These are as follows:

1. All insurers shall have their systems and process audited at least once in three years by a CA firm.
2. In doing so, the current internal or concurrent or statutory auditor is not eligible for appointment.
3. CA firm must be having a minimum of 3-4 years experience of IT systems of banks or mutual funds or insurance companies.

(ii) Preliminaries

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

- i. Location(s) from where Investment activity is conducted.
- ii. IT Applications used to manage the Insurer's Investment Portfolio.
- iii. Obtain the system layout of the IT and network infrastructure including: Server details, database details, type of network connectivity, firewalls other facilities/ utilities (describe).
- iv. Are systems and applications hosted at a central location or hosted at different office?
- v. Internal circulars and guidelines of the Insurer. Standard Operating Procedures (SOP).
- vi. List of new Products/funds introduced during the period under review along with IRDA approvals for the same.
- vii. Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.
- viii. IRDA Correspondence files, circulars and notifications issued by IRDA.
- ix. IT Security Policy.
- x. Business Continuity Plans.
- xi. Network Security Reports pertaining to IT Assets.

(iii) System Controls: These are as follows:

1. 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.
2. 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.
3. 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.

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:

- 1) To regulate the issue of banknotes,
- 2) To maintain reserves with a view to securing monetary stability, and
- 3) To operate the credit and currency system of the country to its advantage.

IS audits are gaining importance as key processes are automated or enabled by technology. 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.

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
- 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) The IS Audit should be independent of the auditee, both in attitude and appearance. The Audit Charter or Policy, or engagement letter (in case of external professional service provider), should address independence and accountability of the audit function.
- d) 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.
- e) *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 Certified Information Systems Auditor (CISA, offered by ISACA), Information Systems Audit (ISA, offered by ICAI), or Certified Information Systems Security Professional (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.
- f) 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 (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).
- g) 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.
- h) IS Auditors should review the following additional areas that are critical and high risk such as:
 1. IT Governance and information security governance structures and practices implemented by the Bank.
 2. Testing the controls on new development systems before implementing them in live environment.
 1. A pre-implementation review of application controls, including security features and controls over change management process, should be performed to confirm that:
 2. Controls in existing application are not diluted, while migrating data to the new application
 3. Controls are designed and implemented to meet requirements of a bank's policies and procedures, apart from regulatory and legal requirements

4. Functionality offered by the application is used to meet appropriate control objectives
3. A post implementation review of application controls should be carried out to confirm if the controls as designed are implemented, and are operating, effectively
4. 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.
5. 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.
6. 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.
7. When IS Auditors believe that the bank has accepted a level of residual risk that is inappropriate for the organization, they should discuss the matter with appropriate level of management.

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:

1. The issuers of securities,
2. The investors, and
3. 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.

(i) 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.

(ii) Audit Report Norms: These are given as follows:

- i. 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.
- ii. 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.

(iii) Auditor Selection Norms: There are various norms for selection of Auditors, which are given as follows:

- i. 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).
- ii. 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.
- iii. The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.
- iv. 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.
- v. 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.

(iv) 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.

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. To understand the term better, an understanding of the independent words will be useful. 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.

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.

Increasing frauds across the cyber space, the sheer size, speed and value of the frauds has surprised the law keeper's. Fraudsters are always on the look-out to misuse any loop hole or weaknesses in the computer systems. Cyber Frauds across the world as withdrawal of an amount equal to USD45 Million, by using ATM cards of banks, sent shock waves across the IT security agencies. There is an increasing demand for experts in the field of cyber forensics. The IT Act under Section 43A and Section 65 to 67B lists various types of cyber-crimes and specifies penalty for them. For example, section 65 has already been discussed in earlier sections.

Keeping the importance of the same in view, the Institute of Chartered Accountants of India, New Delhi, has also launched a post qualification course on the above subject by the name "Certificate Course on Forensic Accounting and Fraud Detection." This post qualification course can be taken by a qualified CA.

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.

The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence to secure cyber space. Major objectives of this policy are given as follows:

- A. 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;
- B. To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem;
- C. To enhance and create National and Sectorial level 24*7 mechanisms for obtaining strategic information regarding threats of ICT infrastructure.
- D. To improve visibility of the integrity of Information & Communication Technology products & services and establishing infrastructure for testing & validation of security of such products;

- E. To create a workforce of 500,000 professional skilled in cyber security in the next 5 years through capacity building, skill development and training;
- F. To provide fiscal benefits to businesses for adoption of standard security practices and processes;
- G. 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;
- H. To enable effective prevention, investigation and prosecution of cybercrime and enhancements of law enforcement capabilities through appropriate legislative intervention;
- I. To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy;
- J. To develop effective public private partnerships and collaborative engagements through technical and operational and contribution for enhancing the security of cyberspace and
- K. 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 in compliance of security.

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.

How the standard works?

ISO 27001 requires that management:

- i. *systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;*
- ii. *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*
- iii. *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.*

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.

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). It encompasses people, processes and IT systems.

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.

Four phases of ISMS: ISO 27001: 2005 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.

PDCA cyclic process :

- 1) **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).
- 2) **The Do Phase** – This phase includes carrying out everything that was planned during the previous phase.
- 3) **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.
- 4) **The Act Phase** – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

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 the organization.

Benefits of ISO 27001

The key benefits of ISO 27001 are given as follows:

- 1) It can act as the extension of the current quality system to include security.
- 2) It provides an opportunity to identify and manage risks to key information and systems assets.
- 3) Provides confidence and assurance to trading partners and clients; acts as a marketing tool.

Structure

In the new structure, the Processing Approach, used in ISO27001:2005, and 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. There are other approaches, and organizations are now free to use them if they wish. The introduction also draws attention to the order in which requirements are presented, stating that the order does not reflect their importance or imply the order in which they are to be implemented.

ISO27001:2013 has ten short clauses, plus a long Annex, which covers the following:

Clause 1: Scope
Clause 2: Normative references
Clause 3: Terms and Definitions
Clause 4: Context of the organization
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement

Standard on Auditing 402: Audit Considerations Relating to an Entity using Service Organization, 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

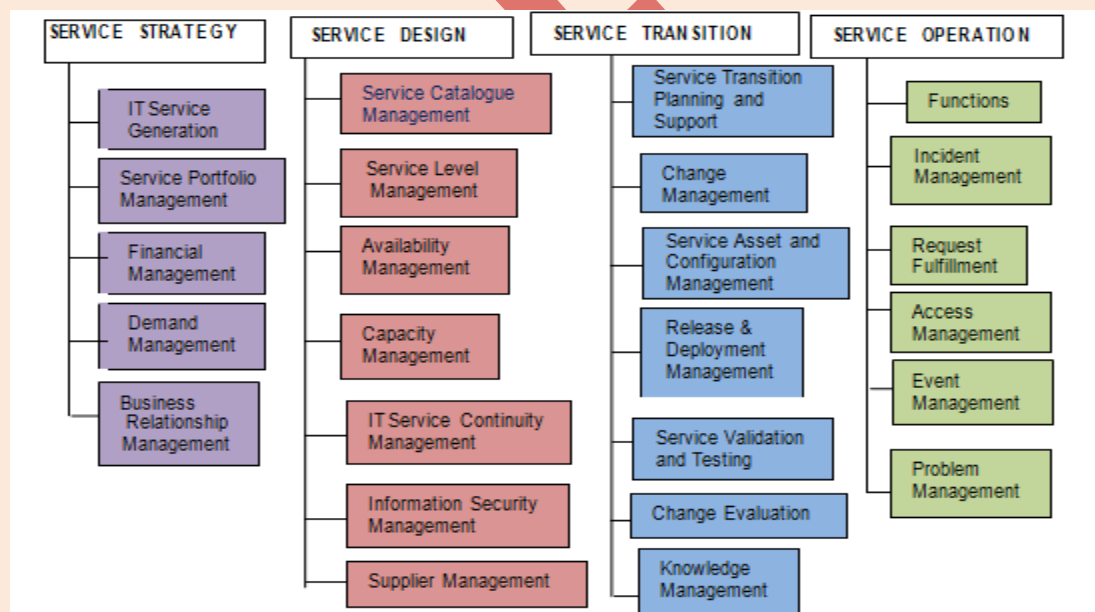
auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations.

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.

ITIL (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 and are 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 competence. It is used to demonstrate compliance and to measure improvement.

It also brought a rationalization in the number of volumes included in the set.

1. **Service Strategy:** This provides guidance on clarification and prioritization of service-provider investments in services;
2. **Service Design:** This provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort;
3. **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);
4. **Service Operation:** This provides best practice for achieving the delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the SLAs).



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.