Chapter 7: Information Technologies Regulatory Issues

7.1 The IT Act and its Objectives

May 2012/Nov 2007/May2005/ May 2003- ***Write a short note on objectives of IT act,2000.***

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**; 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.
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.**

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

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

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

7.2 Key Definitions

Old Practice Manual: Adjudicating Officer: It means an adjudicating Officer appointed under sub-section (1) of section 46.

Nov 2004- Define "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**.

7.3 Digital Signature and Electronic Signature# [Chapter-II]

Old Practice Manual: ***What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature? OR How does the Information Technology (Amendment) Act 2008 enable the authentication of records using digital signatures?***

This chapter of IT Act contains section 3 & 3A.
Section 3 **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. (INTEGRITY & AUTHENTICATION)**

INTEGRITY: 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.**
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.

AUTHENTICATION: 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.
Such identity can be verified by anybody who has the public key# corresponding to such private key#.
This will enable a person who has a public key to identify the originator of the message. The provisions of this section are given as follows:

Classwork:

#**"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.

#**"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.

#**"Subscriber"** means a person in whose name the Electronic Signature Certificate is issued.

#**"Nov 2004- Define Private Key"** means the key of a key pair# used to **create** a digital signature;
#**" Nov 2004- Define Public Key"** means the key of a key pair used to **verify** a digital signature and

listed in the Digital Signature Certificate.

#" **Nov 2004- Define Affixing digital signature"** with its grammatical variation and cognate expression means **adoption of any methodology** or procedure by a person **for the purpose of authentication** of an electronic record and include digital signature.

#**"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.

***[Section 3]* Authentication of Electronic Records:**
Any subscriber may **authenticate an electronic record by affixing his Digital Signature#.**

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.**

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

Explanation -
For the purposes of this section, **"Hash function" means an algorithm mapping or translation of one sequence of bits into another,** generally smaller, set known as "Hash Result" **such that** an **electronic record yields the same hash result every time the algorithm is executed with the same electronic record** as its input **making it computationally infeasible**

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

#**"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.**

#**"Nov 2004/May 2010-Define 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.

***[Section 3A]* Electronic Signature**
Notwithstanding anything contained in section 3, a **subscriber may authenticate any electronic record by such electronic signature*(ES)* or electronic authentication technique*(EAT)*** which- ~~(Flashback: electronic record may be authenticated by means of affixing digital signature.~~)

(a) is considered **reliable**; and
(b) may be **specified in the Second Schedule**

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

a. the **signature creation data***(for ES)* **or the authentication data***(for EAT)* 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.**

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** if such signature or technique is consider reliable.

Every notification issued above shall be laid before each House of Parliament.

7.4 Electronic Governance [Chapter III]

Nov 2009: ***How does the Information Technology (Amendment) Act 2008 enable the objective of the Government in spreading e-governance? OR Discuss the main provisions provided in Information Technology (Amendment) Act 2008 to facilitate E-governance.***

(Answer from section 4 to section 8)

Class work: Exhaustive Revision chart for section 4 to section 10A

This chapter **specifies the procedures to be followed for sending and receiving of electronic records** and the time and the place of the dispatch and receipt.

[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) remains accessible so as to be usable for a subsequent reference.

[#] **May 2010 Define: "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.

[Section 5] Legal recognition of Electronic Signature

Where any law provides that information or any other matter shall be authenticated by affixing the signature[#] **or any document should 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 digital signature affixed **in such manner as may be prescribed by the Central Government.**

[#]**"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.

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

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.

The appropriate Government[#] may 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).

[#]**"Appropriate Government"** means as respects any matter.
(i) enumerated in List II of the Seventh Schedule to the Constitution;
(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and
(iii) in any other case, the Central Government.

[Section 7] Retention of Electronic Records[#]

May 2012: What do you mean by the term electronic record? What are the provisions relating to retention of electronic record in IT act?

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, -**

(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**:

Exceptions:
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.

Nothing in this section **shall apply to any law that expressly provides for the retention of documents,** records or information **in the form of electronic records**, publication of rules, regulation, etc. in Electronic Gazette.

#**"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.

#**"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.

[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.**

[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:**

However
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

May 2012: Briefly explain the power of central government to make rules with respect to the Section 10 of Information Technology (Amendment) Act 2008.

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

Classwork:

(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.**

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

Chapter V sets out the conditions that would apply to qualify electronic records and digital signatures as being secure.

[Section 14] Secure Electronic Record

Section 14 provides **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.**

Classwork:

[Section 15] Secure Electronic Signature

Nov 2010: What do you say about secure electronic record in section 15?

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

(i) The **signature creation data**, at the time of affixing signature, was **under the EXCLUSIVE**

CONTROL of signatory and no other person; and
(ii) The **signature creation data** was **STORED AND AFFIXED IN SUCH EXCLUSIVE MANNER** as may be prescribed.

Explanation *- In case of digital signature, the "signature creation data" means the private key of the subscriber*

7.6 Penalties and Adjudication [Chapter IX]

Old Practice Manual:

Explain with reference to "Information Technology (Amendment) Act 2008":
(Ans: Section 43 to Section 45)
Chapter IX contains sections 43 to 45.
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.

[#]**"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[#].

[#]**"Computer System"** MEANS **a device or collection of devices**,
INCLUDING input and output support devices and
EXCLUDING calculators which are not programmable.

[#]**"Nov 2004 Define Computer Network"** means the **interconnection of** one or more Computers or Computer systems or Communication device through-

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

- Terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained.

Section 43: Penalty for damage to computer, computer system or network

Section 43 deals with penalty for damage to computer, computer system, etc by any of the following methods:

(a) **securing access** to the computer, computer system or computer network;

(b) **downloading or extracting any data**, computer database or information from such computer system or those stored in any removable storage medium;

(c) **introducing any computer contaminant or computer virus** into any computer, computer system or network;

(d) damaging any computer, computer system or network or any computer data, database **or programme;**

(e) **disrupting** any computer, computer system or network;

(f) **denying access to any person authorized to access** any computer, computer system or network;

(g) **providing assistance** to any person **to access** any computer, computer system or network **in contravention of any provisions of this Act** or its Rules;

Explanation.- For the purposes of this section,-
(i) **May 2010 Define-"computer contaminant"** means any **set of computer instructions** that are designed: *(ya toh destroy karne k lie design kia ya fir normal operations ko disrupt karne k lie)*
(a) **to modify, destroy, record, transmit data or programme** residing within a computer, computer system or computer network; or
(b) by any means to **disrupt the normal operation** of the computer, computer system, or computer network.

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

Section 44 states that 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 in the regulations fails to file, return or furnish the same within the time specified 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 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.**

***[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.**

7.7 Offences under IT Act [Chapter XI]
The Computer crimes that are recognized by the Act could affect:
- Hackers
- Digital Contract parties

- Netizen *(Internet+Citizen-Users of Internet*
- Web Site owners/Content creators
- Software professionals
- Auditors
- 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 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.**

FlashBack: **"Computer Source code"** means the **listing of** programmes, computer commands, design and layout and programme analysis of computer resource **in any form.**

***[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,-

(a) Any information that is **grossly offensive or has menacing***(frightening)* **character**; or

(b) Any information which he knows to be false, but **for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury**, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device[#];

(c) 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.

[#]**"Addressee"** means a person who is intended by the originator to receive the electronic record but does not include any intermediary[#].

[#]**"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.

[##]**"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[$].

[$]**May 2010 Define-"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.

[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 personation# by using computer resource

 # Personation is a term used in law for the specific kind of voter fraud where an individual votes in an election, whilst pretending to be a different elector.

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.**

[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**

May 2013: Mr.A has received some information about Mr.B on his cell phone. He knows that this information has been stolen by the sender. He not only retained this information but also send sit to Mr.B and his friends.
Mr.B seek you advice, under which section of IT act he can file FIR with police?
Advice Mr.B detailing the applicable sections.

Answer:

[Section 66A] Punishment for sending offensive messages through communication service, etc.
[Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device
[Section 66E] Punishment for violation of privacy

[Section 66F] Punishment for cyber terrorism

(1) Whoever 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 –**

(jo authorized ha usko access nai de k khud access lene ki try kare ya fir koi contaminent introduce kare)

(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 authorisation 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

(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** 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

***Old Practice Manual:** Briefly explain the Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form as per Section 67 A of the Information Technology (Amendment) Act 2008.*

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

(d) **Facilitates abusing** children online; or

(e) **Records in any electronic form** own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to **five years and with 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**.

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

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.

Any intermediary who intentionally or knowingly contravenes this provisions 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 Controller to give directions

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.

Any person who intentionally or knowingly fails to comply with any such order 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

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 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.

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

The **subscriber or intermediary** or any person in charge of the computer resource **shall**, when called upon by any agency appointed as above **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.

The subscriber or intermediary or any person **who fails to assist the agency** 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

Strike through implies same content as above.

~~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 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.

~~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.~~

~~The intermediary who fails to comply with the direction issued shall be punished with an imprisonment for a term which may extend to seven years and 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, 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.

Explanation: For the purposes of this section,
[#]**May 2010 Define-"computer contaminant"** means any set of computer instructions that are designed:
to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
by any means to disrupt the normal operation of the computer, computer system, or computer network;

[#]***May 2010 Define:"traffic data"*** means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

[#]***"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.

[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.**

[#]**"Critical Information Infrastructure"** means the computer resource, the incapacitation or destruction of which, shall have debilitating*(unbearable)* impact on national security, economy, public health or safety.

(2) The **appropriate Government may,** by order in writing, **authorise the persons who are authorised to access protected systems** notified above.

(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.**

[Section 70A] National nodal agency

(1) The Central Government ~~(APPROPRIATE GOVERMENT)~~ **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 as above **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 above **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** ~~(APPROPRIATE GOVERMENT)~~ 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** 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) such other functions relating to cyber security **as may be prescribed.**

(5) The **manner of performing functions and duties** of the agency **shall be such as may be prescribed.**

(6) For carrying out the provisions of this act, the **agency may call for information and give**

direction to the service providers, intermediaries, data centers, body corporate and any other person.

(7) Any service provider, intermediaries, data centers, **body corporate or person who fails to provide the information called for or comply with the direction** 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.**

#**"Indian Computer Emergency Response Team"** means an agency established under sub-section (1) of section 70 B "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.

[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 there 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.**

[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**,

(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 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.**

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

Chapter XII contains section 79 which provides that the Network Service Providers[#] **shall not 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.**

[#]"network service provider" means an intermediary;

[#] "third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

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

The intermediary will not be liable in following cases:

(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**.

The intermediary will be liable in following cases:

(a) the **intermediary has conspired***(work togather)* or abetted **or aided** or induced whether by threats or promise or otherwise **in the commission of the unlawful act.**

(b) **Even upon receiving information**, 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.

Examiner of Electronic Evidence (CHAPTER XII A)

[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.**

#"Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

7.9 Miscellaneous [Chapter XIII]

[Section 80] Power of Police Officer and Other Officers to Enter, Search, etc.

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

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

The provisions of the Code of Criminal Procedure, 1973 shall apply only to the extent they are related to any entry, search or arrest, made under this section

EXPECTED Q:

[Section 81A] Application of the Act to Electronic cheque and Truncated cheque

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 *by the Central Government*, in consultation with the Reserve Bank of India, *by notification in the Official Gazette*.

Every notification made by the Central Government **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.

(Notification should be laid before each house of parliament for 30 days(30 days is aggregate of one or more sessions)

But agar 30 days se pehle decide hua k notification me kuch change karna ha ya pura hi cancel karna ha toh from that date change or cancellation will be effective but abhi tak jo b hua tha vo sab valid)

[Section 84 C] Punishment for attempt to commit offences*(offence toih commit nai kia but try kia toh offnce karne me jo punishment hota uska 50% punishment)*

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**

Nov 2008- State the liability of companies under section 85 of IT Act.

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: *(company ne offence kia toh vo sab jo responsible the company k conduct k lie vo marenge)*

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.**

However 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. *(but agar koi particular person ki vajah se hua ho ye offence toh baki sab k sath sath ye particular person bhi marenga)*

Explanation-For the purposes of this section

(i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and

(ii) "Director", in relation to a firm, means a partner in the firm

7.10 Requirements of Various Authorities for System Controls & Audit

7.10.1 Requirements of IRDA for System Controls & Audit

The Insurance Regulatory and Development Authority of India (IRDA) is the *apex body overseeing the insurance business* in India.

It *protects the interests of* the policyholders, regulates, promotes and ensures orderly growth of the insurance in India.

Information System Audit 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. *(IS audit hota hi isliye ha ,to comment on CIA)*

It also looks at their efficiency, effectiveness and responsiveness.

It*(Information System Audit)* **focuses on compliance with laws and regulations, which are given as follows:**

(i) System Audit:

These are as follows:

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

(ii) Preliminaries

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

- **Location**(s) from where Investment activity is conducted.

- **IT Applications used** to manage the Insurer's Investment Portfolio.

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

- Are systems and applications **hosted at a central location or** hosted at **different office?**

- **Previous Audit reports and** open issues / details of **unresolved issues** from:
  - Internal Audit,
  - Statutory Audit, and
  - IRDA Inspection / Audit.

- Internal **circulars and guidelines** of the Insurer.

- Standard Operating Procedures **(SOP)** for insurance companies.

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

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

- IRDA Correspondence **files, circulars and notifications issued by IRDA.**

- IT **Security Policy.**

- **Business Continuity Plans.**

- IT **Network Security Reports.**

(iii) System Controls:

These are as follows:

- There should be **Electronic transfer of Data** *without manual intervention*.
- All Systems should be seamlessly *(flawlessly)* integrated.

- Auditor should **REVIEW Audit Trail required at every Data entry point**. Procedures for maintaining and reviewing audit trail should be implemented.

- The auditor should **REVIEW the FOS***(Front Office Module)*, **MOS***(Mid Office Module)* **and BOS***(Bottom Office Module)* **and confirm that the system maintains audit trail** for data entry, authorization, cancellation and any subsequent modifications. (MAINTAINING)

- The auditor should **COMMENT** on the audit trail maintained in the system for various activities*(data entry, authorization, cancellation)*.

• Further, the auditor shall also ascertain that the **system has separate logins for each user and maintains trail of every transaction** with respect to login ID, date and time for each data entry, authorization and modifications.

7.10.2 Requirements of RBI for System Controls & Audit

The Reserve Bank of India (RBI) is India's central banking institution, which **formulates the monetary policy** with regard to the Indian rupee.
The Bank was constituted for the need of following:

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

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.
RBI has been **proactive in providing guidelines on key areas of IT implementation** *by using global best practices.*
They have **constituted various expert committees** *who review existing and future technology and related risks and provide guidelines,* which are issued by all stakeholders.

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. *(internal control jitna effective utna jyada risk managed)*

Some areas of review covered by IS Audit assignments are given here.

(i) System Controls:
These are given as follows:

• Duties of system programmer/designer should not be assigned to persons operating the system and there should be **separate persons dedicated to system programming/design**. 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.**

• **Contingency plans/procedures** in case of failure of system should be **introduced**/ tested at periodic intervals. EDP auditor should put such contingency plan under **test during the audit** for evaluating the effectiveness of such plans.

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

• In order to bring about uniformity of software used by various branches/offices there should be a **formal method of incorporating change in standard software** and it should be approved by senior management. Inspection and **Audit Department should verify such changes from the view-point of control** and for its implementation in other branches in order to maintain uniformity.

• **Board of Directors and senior management are responsible for ensuring** that an institution's

system of **internal controls operates effectively.**

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

• With a view to provide assurance to 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.

(ii) System Audit:

Relevant points are given as follows:

• In banks, **IS Audit should be a separate function within an Internal Audit department** led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE).

• **Banks can leverage 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. *(bahar k auditor ko bulaya toh bhi responsibility for getting an audit done lies with CAE)*

• Because the IS Audit is an integral part of the Internal Auditors, **auditors will also be required to be independent, competent and exercise due professional care.**

• The IS Audit should be **independent** of the auditee, **both in attitude and appearance**. The **Audit Charter or Policy, or engagement letter (in case of external professional service provider), should address independence and accountability of the audit function.**

• Additionally, **to ensure independence** for the IS Auditors, Banks should **make sure that:**
  - Auditors **have access to information and applications**, and
  - Auditors have the **right to conduct independent data inspection and analysis**.

• **Competence:**

IS Auditors should be **professionally competent**, having skills, knowledge, training and relevant experience. They should be **appropriately qualified, have professional certifications and maintain professional competence through professional education and training.**

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.

• 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.

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

➢ IT Governance and information security **governance structures and practices** implemented by the Bank.

➢ **Testing the controls on new development systems** before implementing them in live environment.

➢ A **pre-implementation review of application controls**, including security features and controls over change management process, **should be performed to confirm that:**

✓ **Controls in existing application are not diluted**, while migrating data to the new application
✓ Controls are designed and **implemented to meet requirements of a bank's policies and procedures,** *apart from regulatory and legal requirements*
✓ **Functionality offered** by the application is used to **meet appropriate control objectives**

➢ A **post implementation review of application controls should be carried out** to confirm if the controls as designed are implemented, and are operating, effectively.

➢ 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.

➢ IS Auditors may **validate IT risks before launching a product** or service. *(say bank launch NEFT than auditor will first test the IT risk)*

➢ When IS Auditors believes that the bank has **accepted a level of residual risk that is inappropriate** for the organisation, they **should discuss the matter with appropriate level of management.** If the IS Auditors are not in agreement with the decision, regarding residual risk, IS Auditors and Senior Management should report the matter to the Board (or Audit Committee) for resolution.

In addition, RBI has an inspection wing, which does inspection of banking and non-banking financial institutions.

As part of the audit, one of the critical aspects, which have been reviewed are scope, coverage, frequency and report of system audit.
If system audit has not been done, it is considered as non-compliance and reported to the senior management for compliance.
In the case of branch statutory audit, the LFAR has specific questions pertaining to IT areas such as Security/BCP etc., which need to be reviewed by the statutory auditors.

7.10.3 Requirements of SEBI for System Controls & Audit

The Securities and Exchange Board of India (frequently abbreviated SEBI) is the **regulator for the securities market** in India.
SEBI has to be **responsive to the needs of three groups**, which constitute the market:
• The **issuers** of securities,
• The **investors**, and
• The market **intermediaries**.

Mandatory audits of systems and processes brings transparency in the complex workings of SEBI, proves 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.

• The **Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines** issued by SEBI.

• **Stock Exchange/Depository (Auditee) may negotiate** and the **board of the Stock Exchange / Depository shall appoint** the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can **perform a maximum of 3 successive audits**.

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

• The **scope of the Audit may be extended by SEBI**, considering the changes which have taken place during last year or post previous audit report

• Audit has to be conducted and the **Audit report be submitted to the Auditee**. The report **should have specific compliance/non-compliance issues, observations for minor deviations** as well as qualitative comments for scope for improvement. The report should also take previous audit reports in consideration and cover any open items therein.

• 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:

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

• Auditor must have **minimum 3 years of experience** in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit **experience should have covered all the Major Areas** mentioned under SEBI's Audit Terms of Reference (TOR).

• The Auditor 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.

• The Auditor **should have IT audit/governance frameworks and processes conforming to**

industry leading practices like COBIT.

• The Auditor **must not have any conflict of interest** in conducting fair, objective and independent audit of the Exchange/Depository. It should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.

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

(iv) System Controls:
These are given as follows:

• Further, along with the audit report, Stock Exchanges/Depositories are advised to **submit a declaration from the MD/CEO certifying the security and integrity of their IT Systems**.

• A **proper audit trail** for upload/modifications/downloads of KYC data **to be maintained**

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.

7.11 Cyber Forensic and Cyber Fraud Investigation

Cyber forensics is one of **the latest scientific techniques** that have **emerged due to the effect of increasing computer frauds.**
Cyber, means on 'The Net' that is online.
Forensics is a scientific method of investigation 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.**

Increasing frauds across the cyber space, 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 USD 45 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.

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.

The ever-increasing need for the enterprise to implement security is highlighted here:
Q: Why enterprise need to implement security?
• **Maintain information risk at an acceptable level**
• **To protect information against unauthorised** disclosure, unauthorised or inadvertent modifications, and possible intrusions;

• **Ensure that services and systems are continuously available** to internal and external stakeholders, leading to user satisfaction with IT engagement and services.

• **Comply with** the growing number of **relevant laws** and regulations **as well as contractual requirements and internal policies** on information and systems security and protection,

• **Provide transparency** on the level of compliance; and

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****(flexible)* ***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*".

The policy **document highlights the need for security** in the cyberspace **and outlines that cyberspace is vulnerable to a wide variety of incidents**, whether intentional or accidental manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation-states and non-states actors.

Major objectives of this policy are given as follows:

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

• To **strengthen the Regulatory framework** for ensuring a Secure Cyberspace ecosystem;

• To **enhance and create** National and Sectorial level 24*7 **mechanisms for obtaining strategic information regarding threats of ICT infrastructure***(ICT stands for Information and Communications Technology. The ICT infrastructure is an overall name used to describe all the computer and communications hardware and software used to manage clerical,administrative, and management tasks)*

• To **enhance the protection and resilience of Nation's critical information infrastructure** by operating a 24*7 National Critical Information Infrastructure Protection Center(NCIIPC).

• To **create a workforce of 500,000 professional** skilled in cyber security in the next 5 years through capacity building, skill development and training;

• To **provide fiscal benefits to businesses** for adoption of standard security practices and processes;

• To **enable protection of information while in process**, handling, storage & transit so as to Safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft;

• To **enable effective prevention, investigation and prosecution of cybercrime**;

• To **create a culture of cyber security and privacy** enabling responsible user behavior & actions;

• To **develop effective public private partnerships** for enhancing the security of cyberspace and

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

7.12.1 ISO 27001

ISO ek best practice aur standard ha for managing security aur ISMS ek approach ha security ko manage karne k lie.

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).

An ISMS **helps us coordinate all our security efforts** – both electronic and physical – coherently*(reasonably)*, consistently and cost-effectively.

ISO 27001 **defines how to organize information security** in any kind of organization, profit or non-profit, private or state-owned, small or large.

ISO 27001 is for information security; the same thing that ISO 9001 is for quality – it is a **standard written by the world's best experts** in the field of information security and aims to provide a methodology for the implementation of information security in an organization*. (Aisa toh ha nai world k best expert free baithe the toh bana dia- isliye banya because it can provide methodology for implementation)*

It also **enables an organization to get certified**, which means that an independent certification body has confirmed that information security has been implemented in the best possible way in the organization.

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.

Four phases of ISMS:

ISO 27001
prescribes **'how to manage information security through a system of information security management'(ISMS).**

Such a management system consists of four phases that should be CONTINUOUSLY IMPLEMENTED in order to minimize risks to the CIA of information.

These phases are given as follows:

*Code: PDC Act **or** kidnap karne ka PLAN banaya, PLAN IMPLEMENT(DO) kia, CHECK kia k jisko kidnap karna tha usi ko kidnap kia, aur jo kami reh gai vo next ACT of kidnapping me correct kia.*

1. **THE PLAN PHASE –** This phase serves to plan
   - The **basic organization** of information security *(konsa kidnaper kaha khada rahenga)*
   - Choose the appropriate security controls *(from the catalogue of 133 controls)*
   - Set objectives for information security *(kisko kidnap karna ha)*

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.

(remote le k TV pe channel dekho kidnap ho gaya toh news me aa jayenga, purpose apna TV dekhna nai ha monitor karna ha)

4. **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:

1. The Plan phase

The Plan phase consists of the following steps:

- Determining the **scope** of the ISMS; *(Tu kitna likhenga)*
- **Writing** an ISMS Policy*;(Jitna bol raha ha utna likh)*
- Identifying the **methodology for risk assessment***(tune nai likha toh me risk kaise assess karunga (i.e. methodology)* and determining the **criteria for risk acceptance***(aur tune kitna nai likha toh risk ha)*
- Identification of **assets, vulnerabilities and threats***;(nai likha toh I have laptop(asset), kon tuje kida karenga jo tu nai likhenga)*
- Evaluating **the size of risks***;(kitna mota ha vo jisne tuje kida kia)*

Risk= guest

Control= juice

- Identification of **risk treatment options**; *(guest ko treat karne ka option)*
- Selection of **controls for risk treatment**; *(selection of juice)*

Two management approvals:

- Obtaining management approval **for residual risks**;
- Obtaining management approval **for implementation** of the ISMS; and
- **Writing a Statement of applicability that lists all applicable controls**, states which of them have already been implemented, and those which are not applicable.

2. The Do phase

This phase consists of the following activities:

- **Writing** a risk treatment plan. *(likh do how to treat ghar aye mehman, varna bhul jaouge)*
- **Implementing** the risk treatment plan. *(jo plan likha usko implement karo)*
- **Implementing** applicable security controls. *(risk treatment plan implement kar dia so u need control now)*
- **Determining how to measure** the effectiveness of controls *(control implement kia toh vo effective ha ya nai vo b dekhna padenga aur effective nai honga toh training dena padenga)*
- Carrying out awareness programs and training of employees

Two management points:

- Management of the normal operation of the ISMS
- Management of ISMS resources; and

3. The Check phase

This phase includes the following:

- **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.
- **Regular reviews** of the effectiveness of the ISMS
- **Measuring** the effectiveness of controls

(ISMS effective ha ya nai, jab ki control ha toh effective but kitna effective)

Review by auditor:

- **Internal audits** at planned intervals

Review by management:

- **Management reviews** to ensure that the ISMS is functioning and to identify opportunities for improvement;

Incorporate changes required based on review:

- **Updating security plans** in order to take account of other monitoring and reviewing activities; and
- **Keeping records of activities and incidents that may affect the effectiveness** of the ISMS.

(compare this check phase with icai paper checker)

4. The Act phase

This phase includes the following:

- Implementation of identified improvements in the ISMS

Improvements identify kaise hua? Preventive action se…..

- Taking corrective and preventive action; applying own and others' security experiences

Kam kia toh khud ki tariff toh karenge hi, lekin uske pehle ye dekh lene ka k improvement achieve desired objective varna shareholders dat denge.

- Communicating activities and improvements to all stakeholders and
- Ensuring that improvements achieve the desired objectives.

The key benefits of ISO 27001 are given as follows:

Code: Independent review kia toh pata chala ISO 27001 ne current quality system ko aur badha k security bhi include kar dia the tabhi client itne confident the k risk identify ho k manage ho jayenge.

- Allows an **independent review and assurance** to you on information security practices.
- It can act as the **extension of the current quality system** to include security.
- Provides **confidence and assurance to trading partners and clients**.
- It **provides an opportunity to identify and manage risks** to key information and systems assets.

A company may adopt ISO 27001 for the following reasons:

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

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.

7.12.2 SA 402

Audit Considerations Relating to an Entity using Service Organization, SA 402 **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.

7.12.3 ITIL (IT Infrastructure Library) *(Read it from the point of view of service provider say Tata consultancy services)*

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**.
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 and quality of IT services.
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**.

History of ITIL

Although the UK Government originally created the ITIL, it has **rapidly been adopted across the world as the standard for best practice** in the provision of information technology services.

As IT services become more closely aligned*(associated)* and integrated with the business, **ITIL assists in integrating** business and IT services in best possible manner **to provide maximum benefit of IT services to business.**

The key objective of any Service Management is transforming resources into valuable services and ITIL helps to achieve this objective.

The ITIL V3 library consists of following five books:

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

• ***Service Strategy:*** *(key objective: determine strategy to serve customers, determine which service IT organization should offer)*

- 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*(demonstrate)* 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***(at the base)* **the practice of service management** to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.
- **Topics include the development of markets**, service assets, service catalog, and implementation of strategy through the Service Lifecycle; setting objectives and expectations of performance towards serving customers and market spaces, and to identify, select, and prioritize opportunities.
- Assisting an organization to position itself to deal with the costs and risks associated with its service portfolios, establishing both operational effectiveness and distinctive performance.

• ***Service Design:*** *(key objective: design new IT service and also changes and improvement to existing services)*

- Service Design **translates strategic plans and objectives and creates the designs and specifications for execution** through service transition and operations.
- It ***provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners,*** to present feasible service offerings.
- The Service Design volume **provides guidance on the design and development** of services and service management processes.
- It **includes design principles and methods for converting strategic objectives into portfolios**

of services and service assets.

- Service Design is **not limited to new services** and includes the changes and improvements required to maintain or increase value to customers over the lifecycle of services, taking into account the continuity of services, conformance to standards and regulations and achievement of service levels.

- It **also provides guidance on the development of design capabilities** for service management.

• ***Service Transition:*** *(key objective:to build and organize IT services, provides guidelines to convert design into operations)*

- 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.

- Service Transition provides **guidance on managing the complexity of changes to services and service management processes** to prevent undesired consequences whilst permitting for innovation.

- It provides **guidance on transferring the control of services between customers and service providers**.

• ***Service Operation:*** *(key objective:IT services are delivered efficiently and effectively which include fulfilling user requests, fixing system bugs as well as carrying out routine operational task)*

- 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 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 such as managing the availability of services, controlling demand, optimizing capacity utilization, scheduling of operations, and fixing problems.**

• ***Continual Service Improvement:*** *(aims to continually improve efficiency and effectiveness of IT processes and services)*

- Continual Service Improvement provides guidance on the **measurement of service performance through the service life-cycle**, suggesting improvements to ensure that a service delivers the maximum benefit.

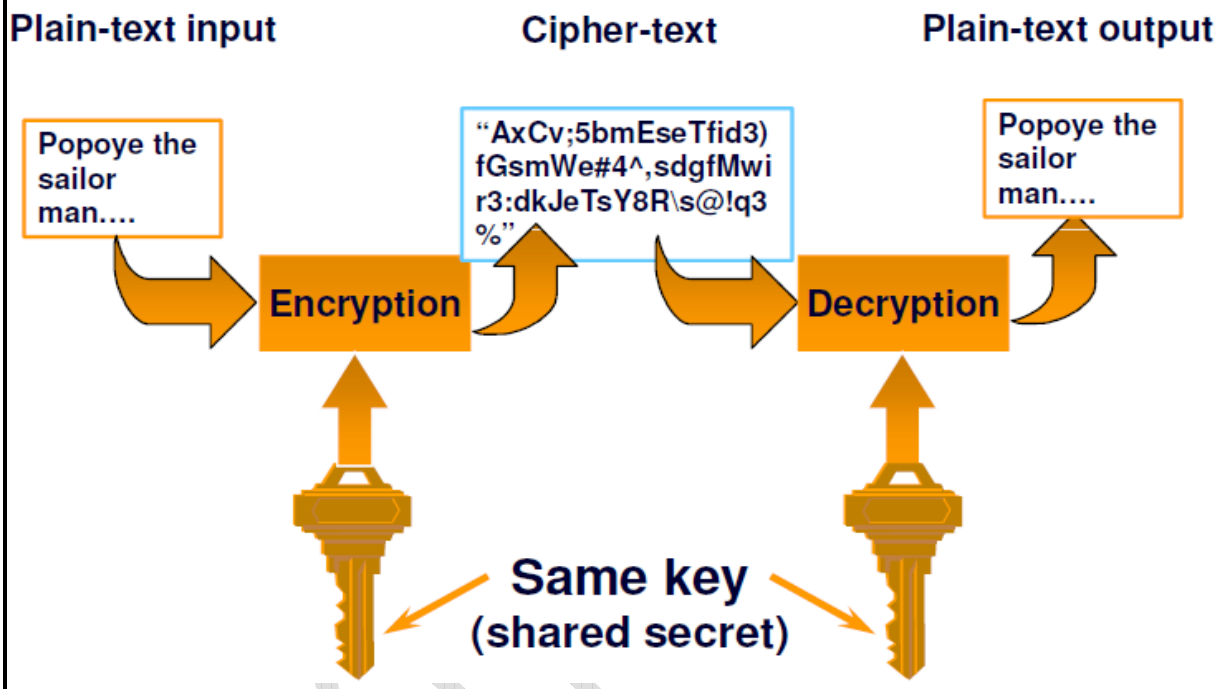
- This volume **provides guidance on creating and maintaining value** for customers through improved design, introduction, and operation of services.

- It **combines principles, practices, and methods** from change management, quality management, and capability improvement **to achieve incremental and significant improvements** in service quality, operational efficiency, and business continuity.

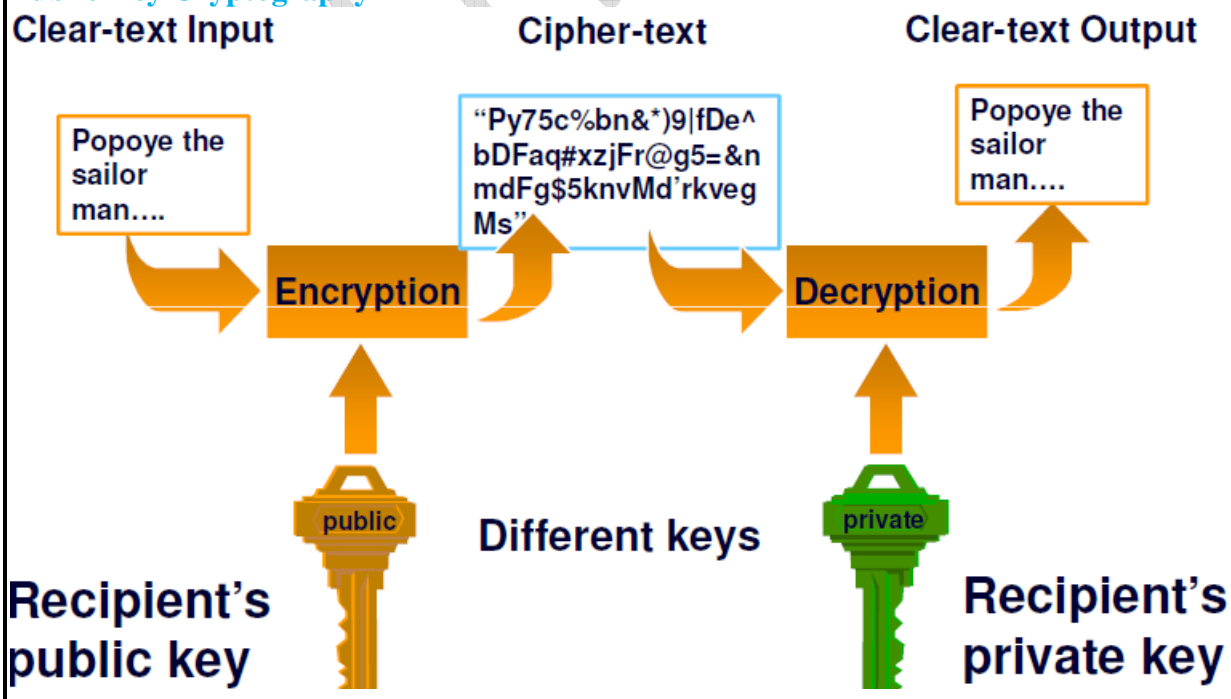
- It **provides guidance on** linking improvement efforts and outcomes with service strategy, design, and transition, focusing on **increasing the efficiency, maximizing the effectiveness and optimizing the cost of services and the underlying IT Service Management processes.**

Some additional ingredients:

Symmetric Key Cryptography

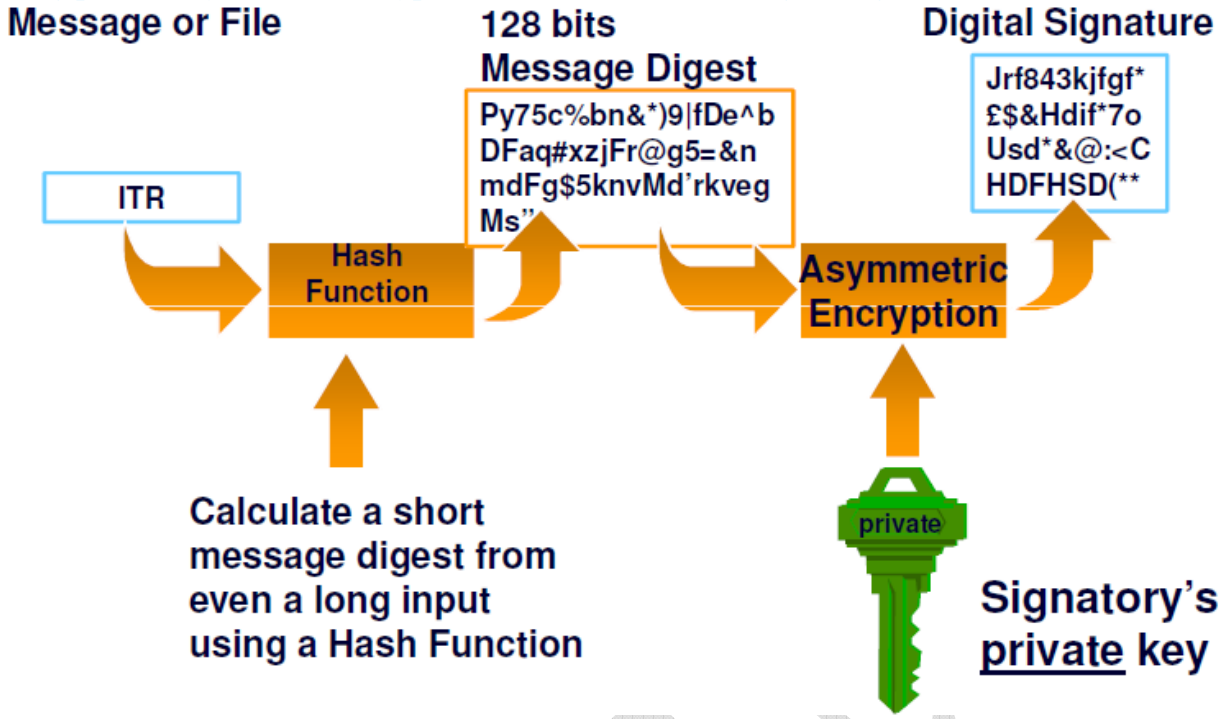


Public Key Cryptography



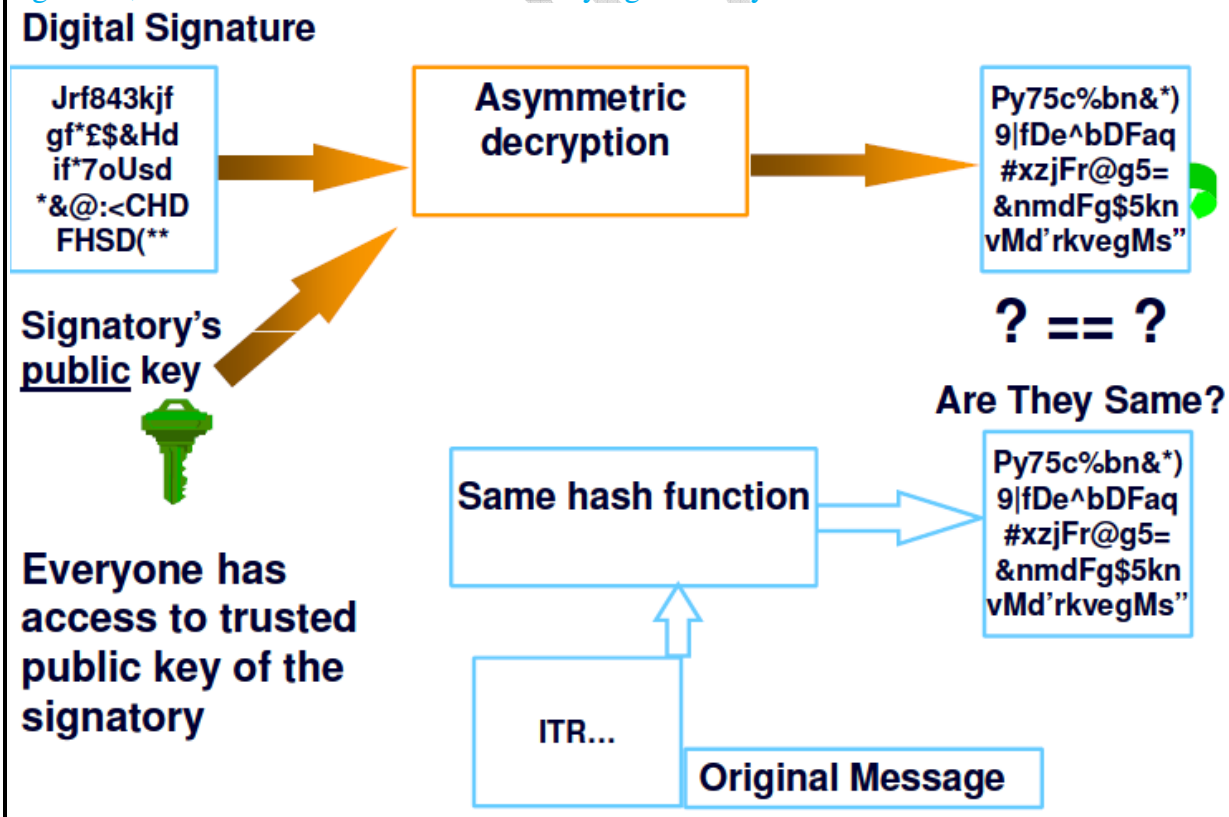
Creating a Digital Signature

Digital signature is a number which is created by use of private key. Message digest is encrypted by using private key and this encrypted number is known as Digital Signature.



Verifying a Digital Signature

The public key is used for verification and it is given to ITD,ROC etc. For transmitting a public key safely to receiver and for providing a proof that public key belong to person who have created digital signature, we obtain a certificate from certifying authority.



In a nutshell, Assessee will send encrypted ITR and Digital Signature to ITD. The ITD creates message digest from both encrypted ITR and Digital Signature and if both message digest are same than it implies message is not changed after transmission and it belongs to the person whose public key is used.

Nov 2006: ***Please read carefully the following three scenarios and answer the questions given below:***

(a) Scenario 1:

Nobody told you that your Internet use in the office was being monitored. Now you have been warned you will be fired if you use the Internet for recreational surfing again. What are your rights?

(b) Scenario 2:

Your employees are abusing their Internet privileges, but you don't have an Internet usage policy. What do you do?

(c) Scenario 3:

Employee Mr. X downloads adult material to his PC at work, and employee Miss Y sees it. Miss Y then proceeds to sue the company for sexual harassment. As the employer, are you liable?

Answer

(a) Scenario 1: When you are using your office computer, you have virtually no rights. You would have a tough time convincing the court that the boss invaded your privacy by monitoring your use of the company PC during office hours. You should probably be grateful that you only got a warning stating that you will be fired if you use the Internet for recreational surfing again.

(b) Scenario 2: Although the law is not fully developed in this area, courts are taking a straightforward approach. If it is a company computer, the company can control the way in which it is to be used by its employees. You really don't need an Internet usage policy to prevent inappropriate use of your company's computer. To protect the company in future, it is advisable to distribute an Internet usage policy to your employees as soon as possible to stop your employees from abusing their Internet privileges.

(c) **Scenario 3:** Whether it comes from the Internet or from a magazine, adult material simply has no place in the office. So Miss Y could certainly sue the company for making her work in a sexually hostile environment. The best defense for the company is to have an Internet usage policy that prohibits employees to access adult sites. Of course, you have to follow-through and monitor. Today, software is available for monitoring the employees whenever they visit adult sites. It will shut down the computer and alert the person who is monitoring Internet usage. If someone is caught browsing adult material in the office, you must at least send a written communication to the offending employee. If the company lacks a strict Internet usage policy, Miss Y could prevail in the Court.