CHAPTER 7

IT Act Objectives:

TBD-SFF

- To give legal recognition for **Transactions** carried out by means of electronic data interchange and electronic commerce in place of paper based methods of communication;
- To give legal recognition for keeping of **Books of accounts by banker's in electronicform**;
- To give legal recognition to **Digital signatures** for authentication of any information;
- To facilitate **electronic storage** of data;
- To facilitate **electronic filing** of documents with Government departments; AND
- To facilitate and give legal sanction to **electronic fund transfers** between banks and financialinstitutions;

CA FINAL

Key Definitions

"**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.

"**Digital Signature**" means authentication of any electronic record by a subscriber bymeansofanelectronicmethodorprocedureinaccordancewith the provisions of section3.

"**Key Pair**", in an asymmetric crypto system, means a private key and its mathematicallyrelatedpublickey,whicharesorelatedthatthepublickeycan verify a digital signature created by the private key.

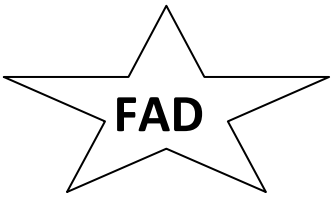
"**Private Key**" means the key of a key pair used to create a digital signature.

Public Key" means the key of a key pair used to verify a digital signature.

***[Section 3]* Authentication of Electronic Records & Section 6**

PENDING: DO IT IN LAST

CHAPTER 7



[Section 7] Retention of Electronic Records

(1) Requirement of laws shall be deemed to have been satisfied regarding retention of documents, records or information in the electronic form, if -

(a) 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;

(b) the information contained therein remains **Accessible** so as to be usable for a subsequent reference;

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

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

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

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

- the **Type** of Electronic Signature;
- any **Other matter** which is necessary to give legal effect to Electronic Signature.
- the manner or **Procedure** which facilitates identification of the person affixing the Electronic Signature;
- **Control processes and procedures** to ensure adequate integrity, security and confidentiality of electronic records or payments; and
- the **Manner and format** in which the Electronic Signature shall be affixed.

CHAPTER 7

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

(c,e,f,g,) includes 'Causes to

If any person **without permission** of the owner or any other person who is in- charge of a **computer, computer system or computer network**,-

(a) **steals or conceals** any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation to the person so affected.

(b) **accesses** to such computer, computer system or computer network or computer resource;

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

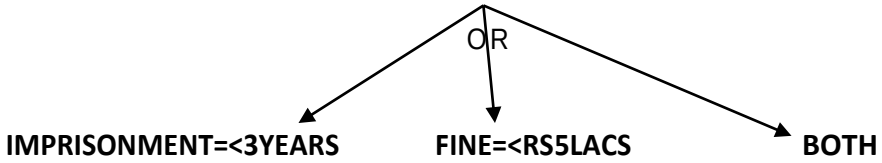
(d) **downloads, copies or extracts any data**, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(e) **damages** any computer, computer system or computer network, computer data base;

(f) **disrupts** of any computer, computer system or computer network;

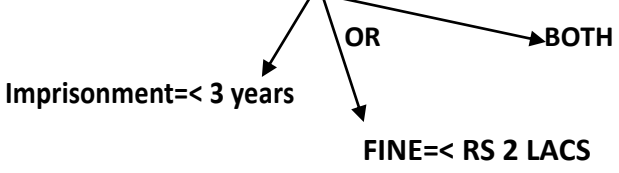
(g) **denies** to any person authorized to access any computer, computer system or computer network by any means;

(h) destroys, deletes or alters any information residing in a computer resource or **diminishes its value** **THEN, PUNISHMENT U/S 66**



[Section65] Tampering with Computer Source Documents

Whoever(*ie by ownself***)** knowingly or intentionally **conceals, destroys or alters or** intentionally or knowingly **causes another** to **conceal, destroy or alter** any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, **shall be punishable**

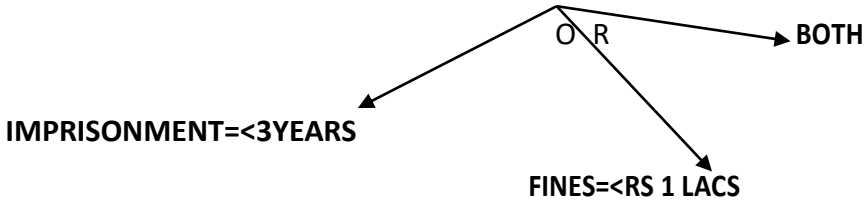


CA FINAL

CHAPTER 7

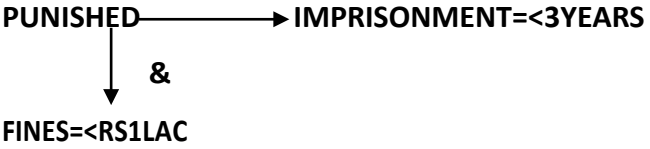
[Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device

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**



[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

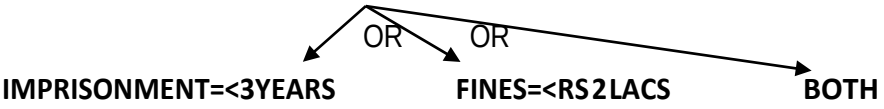


[Section 66D] Punishment for cheating by personation by using computerresource

Whoever, by means of any communication device or computer resource cheats by personating, shall be **punished**

[Section 66E] Punishment forviolation 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**



CA FINAL

CHAPTER 7

[Section 66F] Punishment for cyber terrorism

Whoever knowingly or intentionally **accesses** a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is **restricted** for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with **reasons to believe** that such information, data or computer database so obtained may be used to **cause or likely to cause injury to the interest** of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation to an offence, or **to the advantage** of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism. &
shall PUNISHABLE

May Extend to IMPRISONMENT FOR LIFE

[Section 68] Power of the Controller to give directions

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

(2) Any person who intentionally or knowingly **fails to comply** with any order under sub- section (1) shall be guilty of an offence

IMPRISONMENT=<2YEARS OR **FINES=<RS1LAC** **BOTH**

[Section 70] Protected system

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

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be **punished**

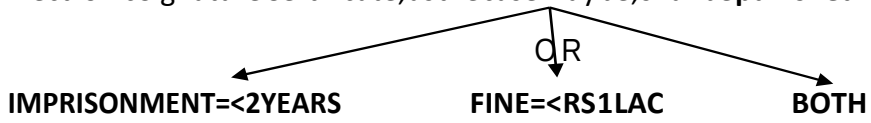
IMPRISONMENT=<10YEARS **&** **LIABLE TO FINE**

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

CHAPTER 7

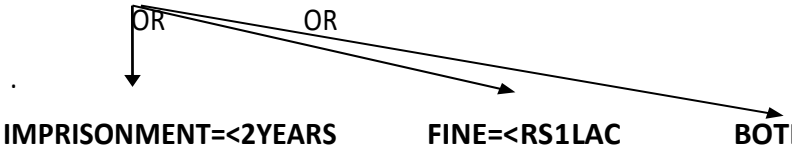
[Section 71] Penalty for misrepresentation

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**



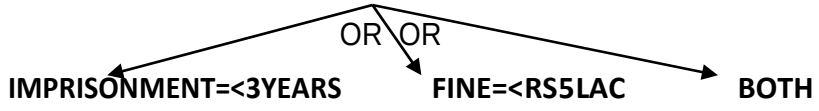
[Section 72] Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be **punished**



[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**



CHAPTER 7

[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**

IMPRISONMENT=<2YEARS OR FINE=<RS1LAC OR BOTH

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

(1) **No person shall publish** an Electronic Signature Certificate or otherwise make it available to any other person **with the knowledge** that -

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

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

(2) Any person who contravenes the provisions of sub-section (1) shall be **punished**

IMPRISONMENT=<2YEARS OR FINE=<RS1LAC OR BOTH

[Section 76] Confiscation

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

Enterprises need to take steps to ensure compliance with cyber laws. Some key steps for ensuring compliance are given below:

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

CHAPTER 7

[Section 84C] Punishment for attempt to commit offences

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which **may extend to one- half of the longest term** of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

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

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 without warrant 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, subject to the provisions of this section, apply, in relation to any entry, search or arrest, made under this section.

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

(1) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.

(2) Every notification made by the Central Government under subsection (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification.

CHAPTER 7

[Section 85] Offences by Companies

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

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

System Auditof IRDA:

- 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.

Systems Audit OF SEBI:

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

  Board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of **3 successive audits**. The proposal from Auditor must be submitted to SEBI for records.
- Audit schedule shall be **submitted** to SEBI **at-least 2 months in advance**, along with scope of current audit & previous audit.
- The **scope** of the Audit **may be extended by SEBI**, considering the changes which have taken place during last year or post previous audit report
- Audit has to be conducted and the Audit report be submitted to the Auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement. The 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.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.

CHAPTER 7

Auditor Selection Norms:

E-IPCC

- 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 should have **IT audit/governance frameworks** and processes conforming to industry leading practices like CoBIT.
- 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.
- 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.
- 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, ETC.

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.

CHAPTER 7

National Cyber Security Policy 2013 Major objectives:

- *To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems;*

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

  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;

  To enable effective prevention, investigation and prosecution of cybercrime;

  To develop effective public private partnerships and collaborative engagements;

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

The Plan-Do-Check-Act (PDCA) cycle

ISO 27001 prescribes 'How to manage information security through a system of information security management'. Such a management system consists of four phases that should be continuously implemented in order to minimize risks to the Confidentiality, Integrity and Availability (CIA) of information.

The PDCA cyclic process is explained below:

- **The Plan Phase (Establishing the ISMS)** – This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
- **The Do Phase (Implementing and Working of ISMS)** – This phase includes carrying out everything that was planned during the previous phase.
- **The Check Phase (Monitoring and Review of the ISMS)** – The purpose of this phase is to monitor the functioning of the ISMS through various **"channels", and check whether the results meet the *set*** objectives.
- **The Act Phase (Update and Improvement of the ISMS)** – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The cycle of these four phases never ends, and all the activities must be implemented cyclically in order to keep the ISMS effective.

CHAPTER 7

Information Technology Infrastructure Library (ITIL)

IT Infrastructure Library (ITIL) is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. Details of the ITIL Framework:

- ***Service Strategy:*** *This provides guidance on clarification and prioritization of service-provider investments in services;*
- ***Service Design:*** *This provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort;*
- ***Service Transition:*** *This elates to the delivery of services required by a business into live/operational use, and often encompasses the "project" side of IT rather than Business As Usual (BAU);*
- ***Service Operation:*** *This provides best practice for achieving the delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the SLAs), and*
- ***Continual Service Improvement:*** *This aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes.*

Service Strategy: SBI-FD

It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

- **Service Portfolio Management:** IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.
- **Business Relationship Management:** Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter -business activities related to providing and consuming knowledge and services via networks.
- **IT Service Generation:** IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process and Information Technology.
- **Financial Management:** Financial Management for IT Services' aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.
- **Demand Management**: Demand management is a planning methodology used to manage and forecast the demand of products and services.

CHAPTER 7

SECTION 3: AUTHENTICATION OF ELECTRONIC RECORDS

- *Electronic Record(ER) is authenticated by Digital Signature(DS) through use of Asymmetric Crypto System & Hash Function.*
- *Any tempering with the contents of ER will immediately invalidate the DS.*
- *Identify of Person affixing DS is authenticated thru use of private key which attach itself message digest & which can be verified by anybody who has public key corresponding to such private key.*
- *Person having public key enabled to identify the originator of the message.*

SECTION 6: USE OF ELECTRONIC RECORDS IN GOVERNMENT & IT'S AGENCIES

RFC

Section 6 provides for use of electronic records in government & it's agencies even though the original law requiring these documents did not provide for electronic forms. It allows use of electronic form for:

- ***R**eceipt or payment of money in Government offices.*
- ***F**iling any form, application or other documents:*
- ***C**reation, retention or preservation of records, issue or grant of any license or permit:*

The appropriate Government has power to prescribe the manner and format of the electronic records.

CA FINAL

CHAPTER 7