CHAPTER 7- INFORMATION TECHNOLOGY REGULATORY ISSUES

1. OBJECTIVES OF THE ACT ARE:

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.
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.

2. DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY

1) A negotiable instrument other than a cheque.
2) A power-of-attorney.
3) A trust.
4) A will or any other document of testamentary nature.
5) Any contract for the sale or conveyance of immovable property or any interest in such property.

3. SECTION 3: AUTHENTICATION OF ELECTRONIC RECORDS

3(1) Electronic record can be authenticated by affixing his Digital Signature
3(2) Authentication is done by the use of asymmetric crypto system and hash function
3(3) Can be verified by public key of the subscriber
3(4) Private key and the public key are unique to the subscriber

Hash Function is an algorithm or formula which generate a unique code called as "Hash Result". The "Hash Result" shall be same for a particular record/file each time Hash Function is applied on that record/file and making following 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.

4. SECTION 3A: ELECTRONIC SIGNATURE (INSERTED VIDE ITAA 2008):

3A Electronic record can be authenticated by electronic signature which –
(a) is reliable and
(b) specified in Second Schedule 3A(2) Electronic signature is reliable if
(a) Signature creation data linked to the signatory
(b) Signature creation data is under the control of the signatory
(c) Alteration to the electronic signature is detectable

(d) Alteration to the information detectable
(e) Fulfills such other conditions as prescribed 3A(3) Central Government may prescribe the details
3A(4) Central Government add to or omit any electronic signature from the second schedule; 3A(5) Notification issued under sub-section (4) shall be laid before Parliament

5. SECTION 4: LEGAL RECOGNITION OF ELECTRONIC RECORDS:

Where any law requires any information in writing / typewritten / printed form, then such information can be –
(a) made available in an electronic form; and
(b) accessible for a subsequent reference

6. SECTION 5: LEGAL RECOGNITION OF ELECTRONIC SIGNATURE:

Where any law requires signature on any document then digital signature can be used in such manner as may be prescribed by the Central Government.
Explanation – For the purposes of this section, "Signed", mean affixing of his hand written signature or any mark on any document

7. SECTION 6: USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURE IN GOVERNMENT AND ITS AGENCIES:

6(1) Where any law provides for –
(a) filing of any form, application or any other document with any Government department
(b) issue of any license, permit, sanction
(c) receipt or payment of money
then, such transactions can be done in electronic form as may be prescribed by the appropriateGovernment
6(2) Appropriate Government may prescribe rules for sub-section (1)

8. SECTION 6A: DELIVERY OF SERVICES BY SERVICE PROVIDER (INSERTED VIDE ITAA-2008):

6A(1) The appropriate Government may authorize any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as notified in Official Gazette.
6A(2) The appropriate Government may authorize to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government.
6A(3) Government may authorize the service providers to collect, retain and appropriate service charges evenif there is no express provision under the Act(say Income Tax Act, 1961), rule etc.
6A(4) Appropriate Government shall specify the scale of service charges which may be charged.

9. SECTION 7: RETENTION OF ELECTRONIC RECORDS:

7(1) A document can be retained in the electronic form. Three conditions -
(a) remains accessible so as to be usable for a subsequent reference;
(b) retained in the format in which it was originally generated, sent or received
(c) origin, destination, date and time of dispatch or receipt are available in the electronic record:

7(2) This section shall not apply to any law where some other provision is there for retention of electronic records.

10. SECTION 7A:

Audit of Documents etc in Electronic form: Applicability of audit on electronic document also.

11. SECTION 8: PUBLICATION OF RULES, REGULATION, ETC, IN ELECTRONIC GAZETTE:

- Government will publish gazette in manual and electronic form also
- Date of notification will be – whichever is earlier

12. SECTION 10: POWER TO MAKE RULES BY CENTRAL GOVERNMENT IN RESPECT OF ELECTRONIC SIGNATURE:

The Central Government may prescribe rules for
(a) type of Electronic Signature
(b) how Electronic Signature shall be attached
(c) how Electronic Signature will be verified
(d) control procedures
(e) any other matter

13. SECTION 43: PENALTY AND COMPENSATION FOR DAMAGE TO COMPUTER, COMPUTER SYSTEM, ETC A PERSON SHALL BE LIABLE TO PAY COMPENSATION IF HE, WITHOUT PERMISSION OF THE OWNER -

(a) accesses computer system
(b) downloads, copies or extracts any data
(c) introduces computer contaminant or computer virus
(d) damages data or computer system or network
(e) disrupts computer system or network
(f) denies access to any authorized person
(g) wrongly charges the services
(h) destroys, deletes or alters any information
(i) Steals or destroys or alters source code

14. SECTION 43A: COMPENSATION FOR FAILURE TO PROTECT DATA

If an organization has any sensitive personal data in its computer resource, then if it is negligent in implementing and maintaining reasonable security controls and thereby causes loss to any person, then such organization shall be liable to pay compensation, to the person so affected.

15. SECTION 44: PENALTY FOR FAILURE TO FURNISH INFORMATION, RETURN, ETC

a) Non-filing of return/document – Upto Rs 1,50,000
b) Late filing – Upto Rs 5000 per day
c) Non-maintenance of books of accounts – Upto Rs 10,000 per day

16. SECTION 45: RESIDUARY PENALTY:

If no penalty has been separately provided for any contravention than residuary penalty upto Rs 25,000 can be imposed

17. OFFENCES

1. ***Section 65:*** Tampering with Computer Source Documents: Imprisonment upto 3 years or fine upto 2 lacks or both.
2. ***Section 66:*** Computer Related Offences as per section 43: Imprisonment upto 3 years or fine upto 5 lacks or both.
3. ***Section 66A***: Sending offensive messages through communication service, etc: Imprisonment upto 3 years and fine.
4. ***Section 66B:*** Dishonestly receiving stolen computer resource or communication device: Imprisonment upto 3 years or fine upto 1 lacks or both.
5. ***Section 66C:*** Identity theft: Imprisonment upto 3 years or fine upto 1 lacks or both.
6. ***Section 66D:*** Cheating by personating by using computer resource: Imprisonment upto 3 years or fine upto 1 lacks or both.
7. ***Section 66E:*** Violation of privacy: Imprisonment upto 3 years or fine upto 2 lacks or both.
8. ***Section 66F***: Cyber terrorism: Upto life imprisonment
9. ***Section 67, 67A, 67B:*** Publishing or transmitting obscene material in electronic form: Imprisonment upto 5 years or fine upto 10 lacks or both.

Section 68 Controller may give directions to a Certifying Authority to take such measures as specified in the order. If any person fails to comply, he shall be liable to imprisonment upto 2 years or fine upto Rs.1 lakhs, or both

Section 69 Power of Central/State Govt to intercept any information on computer network for security reasons

Section 69A Power of Central Govt to block public access of any information through any computer resource for security reasons

Section 69B: Power of Central Govt to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.
"Traffic data" means network logs which can identify origin, destination, route, time, date, size, duration or type of underlying service or any other information

Section 70 empowers the appropriate Government to declare by notification any computer, computer system or computer network to be a protected system. Any unauthorized access of such systems will be punishable with imprisonment which may extend to ten years or with fine.

Section 70B: Indian Computer Emergency Response Team (CERT-In): CERT-In to serve as national agency for incident response:
– Appointed by Central Govt
– Central Govt shall appoint Director General and other officer. Salary and allowances as prescribed.
– Functions of CERT-In in the area of Cyber Security,-

(a) collection, analysis and distribute information on cyber incidents
(b) forecast and alerts of cyber security incidents
(c) emergency measures for handling cyber security incidents
(d) coordination of cyber incidents response activities
(e) issue guidelines, security practices, procedures for prevention of cyber incidents
(f) such other functions as prescribed

– CERT may give order to service providers, intermediaries, data centers, body corporate
– Any person who does not comply with the order shall be punishable with imprisonment upto one year or with fine upto one lakh rupees or with both

Section 71 provides that any person found misrepresenting or suppressing any material fact from the Controller or the Certifying Authority shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both.

Section 72 provides a punishment for breach of confidentiality and privacy of electronic records, books, information, etc. by a person who has access to them without the consent of the person to whom they belong with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both.

Section 73 provides punishment for publishing a Digital Signature Certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both

Section 74 – Publication of electronic signature certificate for fraudulent purpose

If a person knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for fraudulent or unlawful purpose, shall be punished with imprisonment upto 2 years or fine upto Rs 1 lakh or both

Section 75 provides for punishment for commission of any offence or contravention by a person outside India irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Section 76 provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of contravention of any provision of the Act, rules, regulations or orders made there under.

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

1. the function of the intermediary is limited to providing access to a communication system
2. the intermediary does not-
    a. initiate the transmission,
    b. select the receiver of the transmission, and
    c. select or modify the information contained in the transmission
3. observes such other guidelines as the Central Government may prescribe.
4. upon receiving actual knowledge it fails to immediately remove the material.

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

- Any police officer may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or committing any offence under this act

Explanation – Public place includes public conveyance, any hotel, any shop, or any other place intended for use by public

18. ENTERPRISES NEED TO TAKE STEPS TO ENSURE COMPLIANCE WITH CYBER LAWS. SOME KEY STEPS FOR ENSURING COMPLIANCE ARE GIVEN BELOW-

1) Appoint a Cyber law Compliance Officer
2) Conduct regular training of employees on Cyber Laws
3) Implement strict procedures in HR policies for non-compliance
4) Implement authentication procedures as suggested in law
5) Identify and initiate safeguard requirements as applicable under various provisions of the Act such as Sec 43A, 69, 69A, 69B etc
6) Implement security standards
7) Implement reporting mechanism for compliance with cyber laws

19. IRDA REQUIREMENTS FOR SYSTEMS CONTROL & AUDIT

Requirements of IRDA for Systems Control & Audit: The Insurance Regulatory and Development Authority of India (IRDA) has given certain *directions to the insurance companies for Information Systems Audit*. These are as follows

- Audit has to be done at least once in 3 years by a CA firm
- Current internal/concurrent/statutory auditor is not eligible for the appointment
- CA firm must have minimum 3 to 4 years IT audit experience

20. RBI REQUIREMENTS FOR SYSTEMS CONTROL & AUDIT

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.

System Audit of Banks : Few Important points.

- ✓ In this regard, banks require a separate IS Audit function within an Internal Audit department led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE).
- ✓ 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.
- ✓ Qualifications such as Certified Information Systems Auditor (CISA, offered by ISACA), Information Systems Audit (ISA, offered by ICAI), or Certified Information Systems Security Professional (CISSP, offered by ISC2), along with two or more years of IS Audit experience, are desirable.
- ✓ Critical IT general controls such as data centre controls and processes and critical business applications/systems having financial/compliance implications, including regulatory reporting, risk management, MIS systems, etc. needs to be subjected to IS Audit at least once a year (or more frequently, if warranted by the risk assessment).

- ✓ IS Audits should also cover branches, with focus on large and medium branches, in areas such as control of passwords, user ids, operating system security, antimalware, physical security, review of exception reports or audit trails etc.

21. SEBI REQUIREMENTS FOR SYSTEMS CONTROL & AUDIT

Auditor Selection Norms:
i) 3 years experience of IT audit
ii) Auditor qualification- CISA CISM or CISSP
iii) Auditor should follow IT audit framework like COBIT
iv) Auditor should have no conflict of interest
v) Auditor should not have any cases pending against him

22. NATIONAL CYBER SECURITY POLICY 2013

Vision: To build a secure and resilient cyberspace for citizens, business and government.

Mission: To build information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people processes, technology and cooperation

Major objectives of National Cyber Security policy are as follows:-

1. To provide trust & confidence in IT systems and transactions
2. To create an assurance framework and security standards
3. To strengthening the regulatory framework
4. To create National Critical Information Infrastructure Protection Center (NCIIP)
5. To develop suitable indigenous security technologies
6. To improve integrity of IT products and services
7. To create a workforce of 5 lakhs cyber security professionals in next 5 years
8. To promote the adoption of standard security practices and procedures
9. To enable protection of information to safeguard privacy
10. To enable effective enforcement of cyber laws
11. To create a culture of cyber security and privacy
12. To develop public private partnership for enhancing cyber security
13. To enhance global cooperation for cyber security

23. ISO 27001

ISO 27001 is a standard to implement Information Security Management System (ISMS) to managing confidential or sensitive information. Four phases of ISMS -→ PDCA

Plan Phase: The Plan phase consists of the following steps:
- Scope of the ISMS
- Risk assessment
- Identification of assets, vulnerabilities and threats

Do Phase: This phase consists of the following activities:
- Writing a risk treatment plan
- Implementing the risk treatment plan
- Implementing applicable security controls

Check Phase: This phase includes the following:
- Monitoring and reviewing the security activities
- Regular reviews of the effectiveness of the ISMS
- Measuring the effectiveness of controls
- Reviewing risk assessment at regular intervals

Act Phase: This phase includes the following:
- Implementation of identified improvements in the ISMS
- Taking corrective and preventive action
- Communicating activities and improvements to all stakeholders
- Ensuring that improvements achieve the desired objectives.

Key benefits of ISO 27001:

i) Extension of the current quality system to include security
ii) Identify and manage risk to key information and systems assets
iii) Provides confidence and assurance to trading partners and clients
iv) Allows an independent review and assurance on information security practices

Why does a company adopt ISO 27001:

i) Suitable for protecting critical information
ii) Provides a holistic, risk based approach to protect information
iii) Demonstrates credibility and trust with stakeholders, partners and customers
iv) Demonstrates security status as per international standards
v) Increase goodwill and global acceptance of the company

24. ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY)

ITIL is a set of practices for good IT Service Management
Developed by UK Government
ITIL Version 3 is a set of following 5 books: 1. Service Strategy 2. Service Design 3. Service Transition 4. Service Operation, and 5. Continual Service Improvement

1.Service Strategy:

- Strategic management approach in respect of IT Service Management
- Leveraging service management capabilities to effectively deliver value to customers
- Design, development, and implementation of service management
- Principles behind IT service management
- Development of markets, internal and external, service assets, service catalog

2. Service Design:

- Combining infrastructure, applications, systems, and processes, along with suppliers and partners
- Design and development of services
- Increase value to customers, continuity of services, conformance to standards

3. Service Transition:

- Service design and implementation
- switching new and changed services into operations
- Controlling the risks of failure and disruption
- RiskManagement
- Managing the complexity of changes to services
- Transferring the control of services between customers and service providers.

4. ServiceOperation:

- Day-to-day management of IT service
- Supporting operations by means of new models and architectures
- Achieving efficiency and effectiveness in the delivery and support of services
- Ensure value for the customer and the service provider
- Fulfill the strategic objectives
- Detailed guidelines on processes, methods, and tools and fixing problems.

5. Continual Service Improvement:

- Measurement of service performance
- suggesting improvements to service
- Creating and maintaining value for customers
- Combines principles, practices, and methods from change management, quality management, and capability improvement
- Maximizing the effectiveness and optimizing the cost of services