INFORMATION TECHNOLOGY REGULATORY ISSUES

The objectives of the Act are as follows

- Grant legal recognition to transactions carried out by means of electronic means
- Give Legal Recognition for the Digital Signature for authentication of information
- Facilitate E-filing of Documents with the Government Departments
- Facilitate and give legal sanction to Electronic Fund Transfers between Banks and Financial Institutions
- Legal recognition for the keeping of books of accounts by banker's in electronic form

Key issues of electronic information impacting the enterprises and auditors are

- Authenticity:- genuine and authorized transactions
- Reliability:-How to rely on information without physical documents
- Accessibility:- How to gain access and authenticate information in digital form

Authentication of Electronic Records

- Subscriber may authenticate an electronic record by affixing his digital signature
- Authentication shall be effected by use of asymmetric crypto system and hash function
    - Asymmetric Crypto System:-means a system of key pair consisting of private key for creating a digital signature and a public key to verify the digital signature
    - Hash Function:- Algorithm Mapping or translation of one sequence of bits into another such that the electronic record yields the same result each time the algorithm is executed with the same electronic record as input making it computationally infeasible
- Any person by the use of public key of the subscriber cab verify the electronic record
- The Private key and the Public Key are unique to the subscriber and constitute a functioning key pair

Electronic Signature

A Subscriber may authenticate electronic record by electronic signature or electronic authentication technique which is

- Considered Reliable
- Specified in the second schedule

Electronic signature can be considered reliable if

- Signature creation data or authentication data are
  - Linked to the signatory and
  - Under the control of the signatory
- Alteration made to the electronic signature afterwards is detectable
- Alteration to the information made after the affixing of signature is detectable
- Fulfils other conditions as prescribed

Chapter III- Electronic Governance

Section No	Provision
4	Law provides information or matter shall be in writing or typewritten or printed form shall be deemed compliance if • Information is made available in electronic form • Accessible so that is usable for future reference •
5	Law requires information or matter shall be authenticated by affixing a signature deemed to be complied if • Such information is authenticated by electronic signature •
6	Law Providing for • Filing of forms, application or document with office of Govt. • Issue or grant of license or permit or sanction or approval • Receipt or payment of money Deemed to be satisfied if the same is effected by means of electronic form as prescribed
6A	Government may, for efficient delivery of services to public authorise service provider to • setup maintain and upgrade the computerized facilities and perform other services • collect, retain and appropriate the service charges as may be prescribed • Specify scale of Service Charges which may be charged by Service Providers
7	Law Provides for retention of records, documents or information-shall be deemed complied if the same is retained in electronic form • Information remains accessible so as to be usable for subsequent reference • Electronic Record is retained in the format originally generated • Details facilitating identification of origin, destination, date and time of dispatch or receipt of electronic record are available in electronic record
7A	Audit of Documents shall include audit of documents in electronic form also

8	Law Provides for Publication of Rule, Regulation, Bye Law or Notification in Official Notification shall be deemed complied if the same is published in the Electronic Gazette
9	Provisions stated in Section 6,7,8 not confer any right on any person to insist • Any ministry • Department of Central or State Government • Statutory Body • Controlled or funded by the Government To accept, issue, retain, create and preserve any document in electronic form or effect monetary transaction in electronic form
10	Central Government may by rules prescribe • Type of Electronic Signature • Manner of Affixing Electronic Signature • Manner/ Procedure facilitating identification of person affixing the Electronic Signature • Control Processes to ensure the Confidentiality, Integrity and Security of Electronic Records • Other Matter necessary to give legal effect to the Electronic Signature •
10A	In a contract formation if the communication, acceptance, revocation of proposals , expressed in electronic means or through electronic record, contract shall not be deemed to be unenforceable solely on the ground that electronic form was used

Chapter V- Secure Electronic Records and Secure Electronic Signatures

14	Security Procedure applied to the Electronic Record –such electronic Record shall be deemed to be secure electronic record

15	Electronic Signature shall be deemed to be Secure Electronic Signature if
	• Signature Creation Data
	  o At time of affixing signature , was under control of signatory
	  o Stored and affixed in such manner as may be prescribed

16	Central Government may prescribe security procedures and practices

Chapter IX- Penalties, Compensation and Adjudication

43	Any person without the permission of the owner or any person in charge of computer/computer system or network • Accesses or secures access to such • Downloads, copies or extracts any data, including data stored in any storage

	medium • Introduces or causes to be introduced any computer contaminant or computer virus • Damages or causes to be damaged • Damages any programs residing • Disrupts or causes disruption • Denies or causes denial of access to any person authorised to access • Provides assistance to any person to facilitate access in contravention of the provisions of the act • Charges the services availed of by a person to the account of another person by tampering • Destroys, deletes or alters any information residing in any network • Steals, Conceals, destroys or alters or causes any person to do the same with an intention to cause damage
66	Person dishonestly or fraudulently does any act referred to in Section 43, shall be punishable with imprisonment- 3 Years or Fine-Rs.5 Lakhs or both

Computer Contaminant:- Set of Computer Instructions designed to

- Modify, destroy, record, transmit data or programme residing in computer resource
- Usurp the normal operation of computer resource

43A	When a Body Corporate • **Possessing, Dealing or handling** o Any **sensitive personal data or information** in computer resource, which it owns ▪ **Is negligible** in implementing and maintaining **reasonable security practices** • Thereby causing **wrongful loss or wrongful gain** to any person o Shall be **liable to pay damages by way of compensation** to the person so affected
44	Person required to **furnish under this act or regulations** made there under to • **Furnish any document, return or report to the controller of certifying authority** –Penalty not exceeding Rs. 1,50,000 for each failure • **File any return or furnish any information** , books or documents within the time specified in the regulations, shall be liable for a penalty not exceeding Rs.5,000 per day • **Maintain Books of accounts**- Penalty not exceeding Rs .10,000 per day

45	Contravention for which no penalty has been provided separately-Compensation or Penalty not exceeding Rs. 25,000

Chapter XI- Offences

65	Whoever knowingly or intentionally • **conceals, destroys or alters** or **causes another** to do the same to o any **computer source code used as a computer, computer programme**, computer system or computer network, ▪ when the **source code is required to be maintained** under law, • punishable with-**Imprisonment –upto 3 years** or **fine extend to Rs.2 Lakh rupees** or with both
66B	**Dishonestly receives or retains stolen computer resource** or communication device knowing or having reason to believe it is stolen computer resource- • Punishable with Imprisonment -3 Years or Fine extend to Rs.1 Lakh
66C	**Fraudulently or Dishonestly makes use of the Electronic Signature**, Password or any unique identification feature shall be • Punishable with Imprisonment -3 Years or Fine extend to Rs.1 Lakh
66D	Means of a communication device or **computer resource cheats by personating** • Punishable with Imprisonment -3 Years or Fine extend to Rs.1 Lakh
66E	Intentionally or knowingly **captures, publishes or transmits the private area of a person without his or her consent**, under circumstances violating the privacy • Punishable with Imprisonment -3 Years or Fine extend to Rs.2 Lakh
66F	With the intent to threaten the ***Unity, integrity, security or sovereignty of India*** or **strike terror in the people or section** of any people by • **Denying or cause the denial of access** to any person authorised to access computer resource • **Attempting to penetrate or access a computer resource without authorization** or exceeding authorised access or • Introducing or causing to introduce any **computer contaminant** Through such conduct causes or is **likely to cause death or injuries to persons** or damage to **or destruction to property** or **disrupts the supplies** or services essential to the life of the community Knowingly **or intentionally penetrates or accesses a computer resource without authorization** or exceeding authorised access, by such means **obtains access to information**, data or database **which is restricted for the security of state or foreign**

	relations or likely to cause injury to the interests of the sovereignty and integrity of India, security of state, friendly relations with the foreign states, public order, decency or morality, contempt of court, defamation or incitement to an offence , or to advantage of foreign nation, group of individuals or otherwise **commits the offence of cyber terrorism** Whoever **conspires to commit the cyber terrorism** shall be punishable with imprisonment which may **extend to imprisonment for life**
67	Publishes or transmits or causes to be **published or transmitted in electronic form any obscene material –** • Punishable with Imprisonment -3 Years or Fine extend to Rs.5 Lakh (1st Conviction) • Punishable with Imprisonment -5 Years or Fine extend to Rs.10 Lakh (Second or subsequent conviction)
67A	Publishes **or transmits or causes to be publishes or transmitted in electronic form any material containing sexually explicit** act, etc. in electronic form- • Punishable with Imprisonment -5 Years or Fine extend to Rs.10 Lakh (1st Conviction) • Punishable with Imprisonment -7 Years or Fine extend to Rs.10 Lakh (Second or subsequent conviction)
67B	Publishing or transmitting of **material depicting children in sexually explicit act in electronic form** • Punishable with Imprisonment -5 Years or Fine extend to Rs.10 Lakh (1st Conviction) • Punishable with Imprisonment -7 Years or Fine extend to Rs.10 Lakh (Second or subsequent conviction)
67B	Provisions of Section **67,67A and Section 67B not apply to book, pamphlet, paper, writing, drawing and painting** or representation in electronic form • Publication of which is justified as **for the common good –in interest of science, literature art or learning** • Kept for **bona-fide heritage or religious purposes**
67C	Intermediary shall **retain and preserve the information** for the period as prescribed
68	**Controller may** direct **a certifying authority or employee of such authority to take measures or cease carrying on activities** if necessary to ensure compliance with the provisions of the act
69	If the **Central Government of State Government or its authorised officials** find it necessary to do, in the interest of the sovereignty or integrity of India, can direct any **agency of the appropriate Government to intercept, monitor or decrypt any**

	information generated, transmitted, received or stored in any computer resource
69A	If **the Central Government or its authorised officials find it necessary to do**, in the interest of **the sovereignty or integrity of India**, can direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access any information generated, transmitted, received or stored in any computer resource
69B	Central Government **to enhance Cyber Security and for identification**, analysis and **prevention of any intrusion of computer contaminant in the country**, authorise agency of the Government to monitor **or collect traffic data or information generated**, transmitted, received or stored in a computer resource
70	Appropriate Government shall **declare any computer resource directly** or indirectly affects **the facility of Critical Information Infrastructure to be a protected system** and also authorise the persons who are authorised to access the same **Critical Information Infrastructure** means **computer resource-the incapacitation or destruction** of which shall have an impact on the **national security, economy, public health or security**
70A	Central Government, by notification in the Official Gazette, **designate any organisation of the Government as National Nodal Agency** in respect of Critical Information Infrastructure Protection
70B	Central Government, by notification in the Official Gazette, appoint an agency of the Government to be called the **Indian Computer Emergency Response Team** **Indian Computer Emergency Response Team** shall serve as the **National Nodal Agency** for performing the following functions in the Cyber Security arena • Collection, Analysis and dissemination **of information on Cyber incidents** • **Forecasts and alerts** of **cyber security incidents** • **Emergency measures** for handling cyber security incidents • **Coordination** of Cyber incident response activities • **Issue Guidelines, advisories, vulnerability** notes and whitepapers relating to information security practices
71	Whoever **misrepresents or suppresses a fact to the Controller or the Certifying Authority** for obtaining license for obtaining Electronic Signature Certificate shall be • Punishable with Imprisonment -2 Years or Fine extend to Rs.1 Lakh or both
72	Any person who has secured **access to electronic record, book, register, correspondence, information**, document or any other material **without the consent of the person** concerned **discloses such information** to any other person

	• Punishable with Imprisonment -2 Years or Fine extend to Rs.1 Lakh or both
72A	Any **Person including an intermediary** while *providing services under a contract* **has secured access to material** containing **personal information** about another person **with the intent to cause or knowing he is likely to cause wrongful loss** or wrongful gain **discloses such material to any other person** shall be • Punishable with Imprisonment -3 Years or Fine extend to Rs.5 Lakh or both
73	**No person shall publish an Electronic Signature Certificate** or otherwise make it available to any other person **with knowledge** that • **Certifying authority listed in the certificate has not issued it** • **Subscriber listed in the certificate** has **not accepted it** • Certificate has been **revoked or suspended**
74	**Creates, Publishes or makes available Electronic Signature Certificate for any fraudulent or unlawful activity shall be** • Punishable with Imprisonment -2 Years or Fine extend to Rs.1 Lakh or both
75	**Act** shall apply to an offence or contravention committed **outside India by any person irrespective of his nationality** –if the act constituting such offence involves a computer**, computer system or a computer network located in India**
76	**Any Computer, Computer System, floppies, compact disks, tape** drives or accessories related thereto, in respect of **which the provisions of the act has been contravened shall be liable for confiscation**

Steps to be taken by enterprises to ensure compliance with Cyber Laws

- Designate a Cyber Law Compliance Officer
- Conduct Regular training of employees on Cyber Law Compliance
- Implement Strict procedures in HR policy for non-compliance
- Implement Authorisation procedures as suggested in law
- Implement policy and procedures for data retention as suggested
- Implement reporting mechanism for compliance with cyber laws

Chapter XII-Intermediaries not to be liable in certain cases

- Intermediary-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

79	Intermediary **shall not be liable if:-** • Function of intermediary is **limited to providing access to a communication system over which information** made available by third parties is transmitted or temporarily hosted or stored • Intermediary **does not** o **Initiate** the transaction o **Select the receiver** of the transmission o **Select or modify the information contained** in the transmission • **Intermediary observes due diligence** while discharging its duties under the Act Intermediary **shall be liable** • **Intermediary has conspired, or abetted or aided or induced** whether by threats or promise or otherwise in commission of the unlawful act • **On receiving the actual knowledge or being notified by the Government** or agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is used to commit the unlawful act, **intermediary fails to remove or disable access to the material**

Chapter XIII- Miscellaneous

80	**Police officer not below the rank of Inspector or authorised Govt Officer** may enter **a public place and search and arrest without warrant** any person who is suspected **of having committed or committing or being about to commit** any offence under this act Person is arrested by any **person other than the police officer**, **take person to the Magistrate having jurisdiction of the case** or before the officer in charge of a police station
81	Act to have **effect notwithstanding anything inconsistent with the provision of any law** for the time being in force
81A	Provisions of this act **shall apply to electronic cheques and truncated cheques subject to modifications and amendments** necessary for carrying out the purposes of the Negotiable Instruments Act
84B	**Whoever abets an offence ,shall be punishable with the punishment** provided for **the offence** under the act

84C	Whoever **attempts to commit an offence punishable** under the Act or causes such an offence to be committed, **no such provision for punishment for attempt is prescribed**, Punishment shall **be half of the longest term provided for that offence**, with a **fine as provided for offence or both**
85	Person **Committing the offence is a company**, **Every person who was in charge of and responsible to the company** for the conduct of business shall be liable and be proceeded against and punished If Proven **that the contravention took place with the consent of the concerned director**, manager, secretary or any other officer , **they shall also be deemed to be guilty and be proceeded against**

Requirements of Various Authorities for the System and Control Audit

Insurance Regulatory and Development Authority (IRDA)

- System Audit
  - All insurers to have their systems and processes audited once in 3 years by CA Firm-Should not be current internal, concurrent or statutory auditor
  - CA firm to have minimum of 3-4 years of experience of IT systems of Banks or Mutual Funds or Insurance Companies
- Preliminaries
  Auditor to obtain the following information at the audit location
  - Location from where investment activity is conducted
  - IT applications used to manage the Insurer's Investment portfolio
  - Internal Circulars and Guidelines of the Insurer
  - Standard Operating Procedures(SOP)
  - IRDA correspondence files , circulars and notifications issued by IRDA
  - Business Continuity Plans
- System Controls
  - Electronic Transfer of Data without manual intervention –Audit Trail is required at all points
  - Auditor to comment on the audit trails maintained in the system for various activities
  - Auditor to verify that the system has separate logins for each user and maintains trail of every transaction

Reserve Bank of India

- System Controls

- Duties of System Programmer/Developer not to be assigned to the users of the system
- Contingency plans/procedures to be introduced/tested at regular intervals
- Appropriate control measures to be devised and documented to protect the computer system from attacks of unscrupulous elements
- Formal Method of Incorporating change in the Standard Software
- Board of Directors and Senior Management to be responsible for ensuring that the institution of internal controls work effectively
- Annual review of IS audit policy
- Banks to conduct Quality Assurance at least once every three years

- System Audit
  - Banks require a separate IS Audit function within an Internal Audit Department head by an IS Audit head reporting to the Chief Audit Executive
  - IS Audit is an integral part of the Internal Auditors, auditors will be required to be independent
  - IS Audit should be independent of the auditee both in attitude and appearance
  - To ensure independence of auditors banks to ensure that
    - Auditors have access to information and applications, and
    - Auditors have the right to conduct independent data inspection and analysis
  - IS Auditors to be professionally competent , having skills, knowledge and relevant experience
  - IT Governance, Information Security Governance related aspects, critical IT general controls and critical business applications are to be subject to IS audit atleast once a year
  - IS Audits to cover branches, with focus on the medium and large branches, in areas such as control of passwords, user IDs, operating system security, anti malware
  - IS Auditors to review the following additional areas
    - IT Governance and Information Security Governance Structures
    - Testing the Controls
      - Pre-implementation review of application controls
      - Controls in existing applications are not diluted
      - Controls are designed to meet the bank's policy and procedures
      - Functionality offered by the application is used to meet appropriate control objective
  - Post implementation review of the systems to be conducted to confirm if controls as designed are implemented, and are operating effectively
  - Detailed audit of SDLC procedures to confirm that security features incorporated into new system or modifying an existing system are carried out

- Review of processes done by the implementation team to ensure data integrity after the implementation of a new application or system
- IS Auditors may validate the IT risks before launching a product or service
- IS Auditors believe that the bank has accepted a level of residual risk that is inappropriate for the organisation, they should discuss the matter with the appropriate level of management

Requirements of SEBI for Information Systems Control Audit

The Securities and Exchange Board of India (SEBI) hs to be responsive to the needs of three groups in the market

- The Issuers of Securities
- The Investors
- The Market Intermediaries

System Audit

- Audit to be conducted as per the norms prescribed by SEBI
- Audit Schedule-to be submitted to SEBI-at least 2 months in advance ,along with scope of the current and the previous audit
- Scope of the Audit may be extended by SEBI, Considering the changes which have taken place since the last year or previous audit report
- Audit to be conducted and the Audit report is to be submitted to Auditee. Report to have
  - Non-Compliance Issues and
  - Observations for minor deviations, and
  - Qualitative comments for scope for improvement
- Auditee Management Provides their comments about the Non-Conformities and Observations

Audit Report Norms

- System Audit Report and compliance status to be placed before the Governing Body of the Stock Exchanges /Depositories and the system audit report with the comments of the Stock Exchanges or Depositories shall be communicated to SEBI
- Audit Report to have coverage of all the areas outlined in the Terms of Reference (TOR) including any non-conformities or Observations

Auditor Selection Norms

- Auditor to have minimum 3 years experience in IT Audit of Security Industry Participants, e.g. Stock exchanges, clearing houses, depositories etc.

- Auditor to have experience in/direct access to experienced resources in areas covered under TOR
- Auditor should have IT Audit/governance frameworks and processes confirming to the industry leading practices like COBIT
- Auditor not to have conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository
- Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction

System Controls

- Along with the audit report, Stock Exchanges or Depositories are advised to submit a declaration from the MD/CEO certifying the security and integrity of these IT systems
- A proper audit trail for upload/modifications/downloads of KYC Data to be maintained

Cyber Forensics and Cyber Fraud Investigation

- Computer forensics is the **application of investigation** and analysis techniques to **gather and preserve evidence from a particular computing device** in a way that is suitable for presentation **in a court of law**.
- The goal of **computer forensics is to perform a structured investigation** while maintaining a **documented chain of evidence** to find out exactly **what happened on a computing device and who was responsible** for it.

Security Standards

- Information systems security, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.
    - It also refers to: Access controls, which prevent unauthorised personnel from entering or accessing a system.
- Ever increasing need for enterprises to implement security is highlighted here
    - Maintain information **risk at an acceptable level**
    - Ensure that the **services and systems are continuously available** to internal and external stakeholders
    - **Compliance** with the growing rules and regulations
    - Achieving the above by **containing the costs relevant**
- Government recently published the **National Cyber Security Policy**
    - Policy Document highlighted the need for the security in the cyberspace
    - Major Objectives of this policy are as follows
        - Create a Cyber ecosystem in the country-generate adequate trust and confidence in the IT Systems
        - Create assurance framework for design of security policies and for promotion and enabling actions for security

- Strengthen the Regulatory Framework for ensuring a Cyberspace Ecosystem
- To Provide fiscal benefits to the businesses for adoption of the standard security processes and practices
- To enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data
- To create a culture of Cyber Security and privacy enabling the responsible user behaviour and actions through an effective communication and promotion strategy
- Enhance global co-operation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace

ISO 27001

- ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS).
- An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.
- An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.
- It can help small, medium and large businesses in any sector keep information assets secure.
- ISO 27001 requires that management
    - Systematically examines the organisation's information security risks , taking account of threat, vulnerability and impacts
    - Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment
    - Adopts n overarching management process to ensure that the information security controls continue to meet the organisation's information security needs
- ISO 27001 prescribes how to manage Information Security through a System of Information Security Management . Such a management system consists of 4 phases
    - **Plan phase**:- Plan the basic organisation of information security, set objectives for information security and choose the appropriate security controls
    - **Do Phase**:-carrying out everything that was planned during the previous phase
    - **Check Phase**:-Monitor the functioning of ISMS through various channels and check whether the results meet the set objectives
    - **Act:-**The purpose of this phase is to improve everything that was identified as non compliant during the previous phase

ISO 27001:2013

- First Revision of ISO 27001 specifying the requirements for establishing, implementing and maintaining and continually improving an Information Security Management System within the context of the organisation
- It had the following 10 Short Clauses , Covering the following
    - Scope
    - Normative Reference
    - Terms and Definitions
    - Context of the Organisation
    - Leadership
    - Planning
    - Support
    - Operation
    - Performance Evaluation
    - Improvement
- IT specifies 114 Controls in 14 groups. Notable ones being
    - Information Security Policy
    - Organisation of Information Security
    - Asset management
    - Access Control
    - Cryptography
    - Physical and Environmental Security
    - Operations Security
    - Communications Security
    - Relationship with external parties
- Benefits of ISO 27001
    - Act as extension of the current quality system to include security
    - Provides opportunity to identify and manage risks to key information and systems
    - Provides confidence and assurance to trading partners and clients
    - Allows an independent review and assurances on Information Security Practices
- A Company may adopt ISO 27001 for the following reasons
    - Suitable for protecting critical and sensitive information
    - Provides a holistic, risk based approach to secure information and compliance
    - Demonstrates Credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers
    - Creates a market differentiation status according to the Internationally accepted criteria
    - A company which is certified is accepted globally

Standard on Auditing 402 (SA-402)

- SA-402 –Audit Considerations for entity using Service Organisation
- The standard deals with auditor responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organisations

- SA-402 also deals with the aspects like obtaining an understanding of the services provided by a service organisation, including internal control, responding to the assessed risks of material misstatement