7

Information Technology Regulatory Issues

Basic Concepts

1. Information Technology Act, 2000: In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the **Information Technology Act, 2000**. Cyber laws are contained in the IT Act, 2000.This Act aims to provide the legal infrastructure for e-commerce in India and has a major impact for e-businesses and the new economy in India. The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The Act was amended in 2008 by Information Technology (Amendment) Act, 2008.

The provisions of the Information Technology Act 2000 and the amendments of 2008 are simple to understand and most of these are self-explanatory. As an auditor, it is important to understand the key provisions of the IT Act as it impacts and provides the basis for other compliances. For example, when tax audit is being performed and the client accounts are maintained in a computer, it is important for the auditor to know specific provisions and the impact of the data being maintained in electronic form. Further, if audit is being done as per Companies Act, then specific aspects of internal controls and risk management are to be reviewed by auditor.

The Act provides various definitions of different technological terms. The sections, which are found to be relevant and useful for chartered accountants have been covered. For details, candidates are required to refer the Study Material.

2. 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 policyholders, regulates, promotes and ensures orderly growth of insurance industry in India. IRDA has mandated that all insurance companies shall have their systems and processes audited at least once in three years by a Chartered Accountancy Firm.

3. Requirements of RBI for System Controls & Audit: The Reserve Bank of India (RBI) is India's central banking institution, which regulates banking activities in India. IS audits are gaining importance as key processes are automated or enabled by technology. 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. It has constituted various expert committees who review existing and future technology and related risks and provides guidelines, which are issued to 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.

4. Requirements of SEBI for System Controls & Audit: The Securities and Exchange Board of India (SEBI) is the regulator for the securities market in India. SEBI has to be responsive to the needs of three groups, which constitute the market:

- The issuers of securities,
- The investors, and
- The market intermediaries.

Mandatory audit of systems and processes of Stock Exchanges brings transparency in the complex workings, proves integrity of the transactions and builds confidence among stakeholders.

5. Cyber Forensic and Cyber Fraud Investigation: Cyber forensics is one of the latest scientific techniques that has emerged due to the effect of increasing computer frauds. To understand the term better, an understanding of the independent words will be useful. Cyber, means on 'The Net' that is online. Forensics is a scientific method of investigation and analysis techniques to gather, process, interpret, and to use evidence to provide a conclusive description of activities in a way that is suitable for presentation in a court of law. Considering 'Cyber' and 'Investigation' together will lead us to conclude that 'Cyber Investigation' is an investigation method gathering digital evidences to be produced in court of law.

Increasing frauds across the cyber space, the sheer size, speed and value of the frauds has surprised law keepers. Fraudsters are always on the look-out to misuse any loop hole or weaknesses in the computer systems.

6. National Cyber Security Policy 2013: Considering the importance of information security, Government of India recently published the National Cyber Security Policy 2013 with the vision "*To build a secure and resilient 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*".

Based on the key aspects of National Cyber Security Policy 2013, we can understand that Chartered Accountants in their role as accountants and auditors have another important role to play in ensuring compliance of security and also pro-actively provide assurance on the state of IT security in an enterprise.

7. ISO 27001: ISO/IEC 27001 (International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC)) defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large.

ISO/IEC 27001:2005, part of the growing ISO/IEC 27000 family of standards, was an Information Security Management System (ISMS) standard published in October 2005 by ISO/IEC. Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information Security Management Systems – Requirements. It was superseded, in 2013, by ISO/IEC 27001:2013.

An ISMS is a systematic approach to managing confidential or sensitive information so that it remains secure (which means available, confidential and with its integrity intact). It encompasses people, processes and IT systems.

Four phases of ISMS: ISO 27001: 2005 prescribes 'how to manage information security through a system of information security management'. Such a management system, just like ISO 9001 or ISO 14001, consists of four phases that should be continuously implemented in order to minimize risks to the CIA of information.

These phases are given as follows:

- **The Plan Phase –** This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
- **The Do Phase –** This phase includes carrying out everything that was planned during the previous phase.
- **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.
- **The Act Phase –** The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

ISO/IEC 27001:2013 is the first revision of ISO/IEC 27001 that specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System within the context of the organization. It is an information security standard that was published on 25th September 2013. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. ISO 27001:2013 does not put so much emphasis on this cycle.

Structure

In the new structure, the Processing Approach, used in ISO27001:2005, and which houses the PDCA model, was eliminated. The reason for this is that the requirement is for continual improvement and PDCA is just one approach to meeting that requirement. There are other approaches, and organizations are now free to use them if they wish. The introduction also draws attention to the order in which requirements are presented, stating that the order does not reflect their importance or imply the order in which they are to be implemented.

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

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

8. Standard on Auditing 402: Audit Considerations Relating to an Entity using Service Organization, SA 402 is a revised version of the erstwhile Auditing and Assurance Standard (AAS) 24, "Audit Considerations Relating to Entities Using Service Organizations" issued by the ICAI in 2002. The revised Standard deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. SA 402 also deals with the aspects like obtaining an understanding of the services provided by a service organization, including internal control, responding to the assessed risks of material misstatement, Type 1 and Type 2 reports, fraud, non-compliance with laws and regulations and uncorrected misstatements in relation to activities at the service organization and reporting by the user auditor.

9. ITIL (IT Infrastructure Library): ITIL is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. ITIL describes procedures, tasks and checklists that are not organization-specific and are used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure competence. It is used to demonstrate compliance and to measure improvement.

This release of ITIL brought with it an important change of emphasis, from an operationally focused set of processes to a mature service management set of practice guidance. It also brought a rationalization in the number of volumes included in the set, which now comprises

the following:

- **Service Strategy:** 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 value for service providers.
- **Service Design:** 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.
- **Service Transition:** 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.
- **Service Operation:** 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.
- **Continual Service Improvement:** 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.

Question 1

Explain the objectives of the Information Technology Act 2000.

Answer

Major objectives of the Information Technology Act 2000 are given as follows:

- 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;
- To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
- To facilitate electronic filing of documents with Government departments;
- To facilitate electronic storage of data;
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- To give legal recognition for keeping of books of accounts by banker's in electronic form; and

- 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.

Question 2

Define the following terms regarding Information Technology Act 2000:

(i) Digital signature *(ii) Electronic form*

(iii) Key Pair *(iv) Asymmetric Crypto System*

Answer

(i) **Digital Signature:** It 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.

(ii) **Electronic form:** With reference to information, it means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.

(iii) **Key Pair:** In an asymmetric cryptosystem, it 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.

(iv) **Asymmetric Crypto System:** It is a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Question 3

Explain 'Authentication of Electronic Records' with reference to Section 3 of Information Technology Act 2000.

Answer

***[Section 3]* Authentication of Electronic Records:**

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-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.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Question 4

Discuss the main provisions provided in Information Technology Act 2000 to facilitate e-Governance.

Answer

e-Governance sections of chapter III 6, 7 and 8 are the main sections for provisions related to e-Governance provided in Information Technology Act 2000 to facilitate e-governance.

Section 6 lays down the foundation of electronic Governance. It provides that the filling of any form, application or other documents; creation, retention or preservation of records, issue or grant of any license or permit; receipt or payment in Government offices and its agencies may be done by means of electronic form. The appropriate Government has the power to prescribe the manner and format of the electronic records.

Section 7 provides legal sanctity and documents; records or information can be retained in electronic form thus removing the need to retain it in physical form. To safeguard the information even when technology changes, it provides that:

(i) It should be possible to access and use the information later;

(ii) Whenever the original format of the information is changed (e.g. due to technology) the new content should accurately represent the original information; and

(iii) The document should contain details to identify the origin, destinations, dates and time of dispatch or receipt of such electronic record (e.g. when emails or logs are stored).

Section 8 provides that rules, regulations, orders, bye-laws and notifications required under any law to be published in the official Gazette can be published in the electronic gazette substituting the need for manual documents.

Question 5

Discuss the 'Use of Electronic Records in Government and its agencies' in the light of Section 6 of Information Technology Act 2000.

Answer

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

- filing any form, application or other documents;
- creation, retention or preservation of records, issue or grant of any license or permit;
- receipt or payment of money in Government offices.

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

Question 6

Describe the 'Power to make rules by Central Government in respect of Electronic Signature' in the light of Section 10 of Information Technology Act 2000.

Answer

Section 10 gives the Central Government following powers to make rules in respect of Electronic Signature -

(a) specify the type of Electronic Signature;

(b) specify the manner and format in which the Electronic Signature shall be affixed;

(c) specify 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.

Question 7

Describe the 'Tampering with Computer Source Documents' in the light of Section 65 of Information Technology Act 2000.

Answer

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programme, computer commands, design and layout and program analysis of computer resource in any form.

Question 8

Discuss 'Power of the Controller to give directions' under Section 68 of Information Technology Act 2000.

Answer

Certifying Authorities create digital signatures and provide them to subscribers. People use and rely on Digital signatures for carrying on electronic commerce. If signatures are compromised, or if there are insufficient safeguards over their creation or provision, the system will be weakened. To prevent this, the Controller is provided following powers:

[Section 68] **Power of 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 there under.

(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or with both.

Question 9

Discuss 'Power to issue directions for interception or monitoring or decryption of any information in any computer resource' under Section 69 of Information Technology Act 2000.

Answer

Section 69 gives powers to Central & State Governments to issue directions empowering a Government agency to intercept, monitor or decrypt any information through or in any computer if it is for important purposes as specified in the section. These include:

(1) Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), 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.

(2) The Procedure and safeguards over such interception or monitoring or decryption, shall be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by the agency, extend all facilities and technical assistance to -

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist such agency shall be punished with imprisonment up to seven years and fine.

Question 10

Discuss 'Penalty for publishing Electronic Signature Certificate false in certain particulars' under Section 73 of Information Technology Act 2000.

Answer

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

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

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

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

(c) the certificate has been revoked or suspended,

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

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Question 11

What is the vision of National Cyber Security Policy 2013? Also, explain its major objectives.

Answer

Vision of the National Cyber Security Policy 2013 is: "To build a secure and resilient 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".

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 create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology, & people);
- 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 creating scenarios for response, resolution and crisis management through effective predicative, protective, response and recovery actions;
- To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24*7 National Critical Information Infrastructure Protection Center(NCIIPC) and mandating security practices related to the design, acquisition, development and operation of information resources;
- To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, and pilot development of secure ICT products/processes in general and specifically for addressing National Security requirements;
- To improve visibility of the integrity of ICT products & services and establishing infrastructure for testing & validation of security of such products;
- To create a workforce of 500,000 professionals 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 and enhancements of law enforcement capabilities through appropriate legislative intervention;
- To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy;

- To develop effective public private partnerships and collaborative engagements through technical and operational collaboration and contribution 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.

Question 12

Discuss PDCA cyclic process under ISO 27001.

Answer

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

ISO27001 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 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 to keep the ISMS effective. ISO/IEC 27001:2005 applies this to all the processes in ISMS.

Question 13

Discuss the 'Service Strategy' of IT Infrastructure Library (ITIL) Framework.

Answer

Service Strategy: The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service-provider investments in services. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate 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 the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

- **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.
- **Service Portfolio Management:** IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.
- **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.
- **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.

Question 14

Mr. A has hacked into Defense Information Systems with an intention to steal classified information that threatens the security and sovereignty of India. He has used the services of a local cafe, 'CyberNet' for this purpose. The owner of 'CyberNet' tries to stop Mr. A but is threatened by Mr. A. Hence the owner of 'CyberNet' does not disclose A's activities to anyone. Mr. A is caught by the Vigilance Officers of the department.

(i) Is Mr. A punishable for his activities?

*(ii) Is the interm*ediary, 'CyberNet' liable?

Please discuss the liabilities enunciated under the relevant sections of the Information Technology Act, 2000 in the above two cases.

Answer

(i) Yes, Mr. A is punishable for his activities under the Section 66F.

[Section 66F(1)(B)] Punishment for cyber terrorism

Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty

and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

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

Considering the facts provided in the case where Mr. A hacked into Defense Information System with an intention to steal classified information threatening the security and sovereignty of India, Mr. A is punishable for his activities.

(ii) Yes, Intermediary 'CyberNet' is liable under the Section 79.

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

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.

(2) The provisions of sub-section (1) shall apply if -

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(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.

Thus, according to Section 79(2)(c); the Intermediary 'CyberNet' failed to observe due diligence in discharging his duties and also the other guidelines as prescribed by the Central Government. So, Intermediary 'CyberNet' is liable.

Question 15

ABC Ltd. is a security market intermediary, providing depository services. Briefly explain the relevant requirements with respect to annual systems audit mandated by SEBI in this regard.

Answer

SEBI (Securities and Exchange Board of India) 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. 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. 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.

Question 16

The manner of selecting auditors builds confidence among various stakeholders. Describe SEBI norms for selecting an auditor.

Answer

The SEBI norms for Auditor Selection are 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 (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. He 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.

Question 17

Discuss "Authentication of Electronic Records" regarding the Information Technology Act, 2000.

Answer

In Information Technology Act, 2000, Section 3 defines "Authentication of Electronic Records". This section provides the conditions subject to which an electronic record may be authenticated by means of affixing 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. It will also enable a person who has a public key to identify the originator of the message. The provisions stated in the Act are as follows:

Authentication of Electronic Records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair. [Section 3]

Question 18

What is a "Protected System" under the IT Act?

Answer

In IT Act, 2000, Section 70 defines "Protected System" that is as follows:

Protected System

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

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

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

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

Question 19

Describe the provision related to 'Compensation for failure to protect data' under Section 43A and 'Penalty for failure to furnish information return, etc.' under Section 44 of the Information Technology Act, 2000.

Answer

Section 43A of Information Technology Act, 2000 is as follows:

[Section 43A] Compensation for failure to protect data

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Section 44 of Information Technology Act, 2000 is as follows:

[Section 44] Penalty for failure to furnish information return etc.

If any person who is required under this Act or any rules or regulations made there under to -

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore 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.

Question 20

As an IT consultant, your client is seeking your advice whether to go for ISO 27001. Explain the reasons for which company may adopt ISO 27001.

Answer

- *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.*

Question 21

Write the objectives of Information Technology Act, 2000.

Answer

The objectives of the Information Technology Act, 2000 are as follows:

- *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;*
- *To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;*
- *To facilitate electronic filing of documents with Government departments;*
- *To facilitate electronic storage of data;*
- *To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;*
- *To give legal recognition for keeping of books of accounts by banker's in electronic form; and*
- *To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve*

Question 22

How does Information Technology Act, 2000 define the term Electronic Signature? State under what conditions any electronic Signature or Electronic Authentication technique shall be considered reliable as per Section 3A of Information Technology Act, 2000.

Answer

As per Information Technology Act, 2000; the definition of Electronic Signature is as follows:

"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.

[Section 3A (2) of IT Act, 2000] Electronic Signature

Any Electronic Signature or Electronic Authentication technique shall be considered reliable if-

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfills such other conditions which may be prescribed.

Exercise

1. *Briefly explain the following with respect to the Information Technology Act 2000:*
   - *(i) [Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device*
   - *(ii) [Section 66D] Punishment for cheating by personation by using computer resource*
   - *(iii) [Section 66E] Punishment for violation of privacy*
   - *(iv) [Section 66F] Punishment for cyber terrorism*
2. *Explain the 'Power to issue directions for blocking public access of any information through any computer resource' under Section 69A of the Information Technology Act 2000.*
4. *Explain the 'Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security' regarding Section 69B of the Information Technology Act 2000.*
5. *Write short notes on the following:*
   - *(i) [Section 4] Legal Recognition of Electronic Records*
   - *(ii) [Section 5] Legal Recognition of Electronic Signature*
6. *Write short notes on the following:*
   - *(i) System Controls regarding the requirement of RBI for System Control and Audit*
   - *(ii) Auditor Selection Norms regarding the requirement of SEBI for System Control and Audit*
7. *Discuss ITIL framework.*