ISCA

Information System Control and Audit

First Edition: ***January 2015***

Price: Rs. 400/-

Published By: CA BOOK CORPORATION
SILIGURI
Amrit Jaiswal : 9832492295
Sumit Chanani : 9749094848
Email: cabookcorp@gmail.com

Preface

*It gives me immense pleasure to introduce the **1st** edition of this book in the hands of its reader.*

We know that the information system control and audit paper has been revised and updated. The book has been prepared to enable complete and systematic study of the subject in simple understandable language.

Every Chapter has been designed in Question and Answer format. Space has been deliberately left on the sides of every question for the students to write down important points of each answer. This enhances better retention capacity.

I would feel immensely rewarded if students find this book of great help in preparing for their exams.

I express my gratitude to CA Amar Agarwal who has been constant source of inspiration for completion of this book.

This book would not have been complete without the unconditional support of my wife CA Richu Agarwal.

I am also thankful to Sumit Chanani, Ajay Bansal, Amrit Jaiswal who have contributed immensely by devoting their time and effort in completion of this book.

I have made my sincere efforts to make the book more meaningful, comprehensive, and compact and complete but even then there is always space for improvements.

It will be a great pleasure to share your experience with the book and honour your suggestions; you are welcome to write at manoj_y2005@rediffmail.com

1st January, 2015 *With best wishes*

Siliguri *CA Manoj Agarwal*

This is the Sample EBook.

Books are Available at Flat 30% discount.

Students Interested in Buying the books OR for any other Query may Contact:

Sumit Chanani : 09749094848 (Whatsapp)

Amrit Jaiswal : 09832492295 (Whatsapp)

CHAPTER-7

INFORMATION TECHNOLOGY REGULATORY ISSUES

Question 1

Explain briefly the scope of the Information Technology (Amendment) Act 2008 along with the relevant definitions that are used.

Answer

Scope of the Information Technology (Amendment) Act 2008: This Act is meant for whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person. The Act was enforced by the Central Government from October 17, 2000.

The Act shall not apply to the following:

- A **negotiable instrument** as defined in Section 13 of the Negotiable Instruments Act, 1881;
- A **power of attorney** as defined in Section 1A of the Powers- of Attorney Act, 1882.
- **A trust** as defined in Section 3 of the Indian Trusts Act, 1882.
- **A will** as defined in Section (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
- Any **contract for the sale or conveyance** of immovable property or any interest in such property.
- **Any such class of documents** or transactions as may be notified by the Central Government in the Official Gazette.

The Act consists of 94 Sections spread over thirteen Chapters & four Schedules to the Act. The schedules to the Act contain related amendments made in other Acts as outlined in the objectives of the Act, namely, the Indian Penal code, the Indian Evidence Act, 1972, the Banker's Book Evidence Act, 1891 & the Reserve Bank of India, 1934.

Section 2 contains some of the important terms that are defined below:

(a) "**Access**" means gaining entry into, instruction or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network.

(b) "**Addressee**" – a person who is intended by the originator to receive the electronic record but does not include any intermediary.

(c) "**Affixing digital signature**" – adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

(d) "**Appropriate Government**" – Central Government except in the following two cases where it means the State Government.

- In the matters enumerated in List 2of the Seventh Schedule to the Constitution.
- Relating to any state law enacted under List 3 of the Seventh Schedule to the Constitution.

(e) "**Asymmetric crypto system**" means a system of a secure key pair consisting of a private key for creating a digital signature & a public key to verify the digital signature.

(f) "**Computer**" – any electronic, magnetic or optical or other high speed data processing device or system which performs logical, arithmetic, & memory functions by manipulations of electronic, magnetic or optical impulses, & includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

(g) "**Computer network**"- the interconnection of one or more, computers through

(i) The use of satellite, microwave, terrestrial line or other communication media &

(ii) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

(h) "**Computer resource**" – computer, computer system, computer network, data, computer data base or software.

(i) "**Computer system**" – a device or collection of devices including input & output support devices & excluding calculators which are not programmable & capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data & output data, that performs logic, arithmetic, data storage & retrieval, communication control & other functions.

(j) "**Data**" – a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, & is intended to be processed, is being processed or has been processed in a computer system or computer network, & may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

(k) "**Digital signature**" – authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3.

(l) "**Electronic form**" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

(m) "**Electronic record**" –data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

(n) "**Function**" –in relation to a computer, includes logic, control arithmetical process, deletion, storage & retrieval & communication or telecommunication from or within a computer.

(o) "**Information**" includes data, text, images, sound, voice, codes, computer programs, software & databases or micro film or computer generated micro fiche.

(p) "**Intermediary**" with respect to any particular electronic message means any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message.

(q) "**Key pair**", in an asymmetric crypto system, means a private key & its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

(r) "**Originator**" – a person, who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

(s) "**Prescribed**" –prescribed by rules made under this Act.

(t) "**Private Key**" – the key of a key pair used to create a digital signature.

(u) "**Public key**" – the key of a key pair used to verify a digital signature & listed in the Digital Signature Certificate.

(v) "**Secure system**" means computer hardware, software & procedure that

- Are reasonably secure from unauthorized access & misuse.
- Provide a reasonable level of reliability & correct operation.
- Are reasonably suited to performing the intended function &
- Adhere to generally accepted security procedures.

(w) "**Verify**" – in relation to a digital signature electronic record on public key with its grammatical variations & cognate expressions means to determine whether.

- The initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber.
- The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

Question: 2

What are the objectives of IT act 2000?

Answer:

This is an Act to provide legal recognition for transactions carried out by means of electronic data interchange & other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication & storage of information, to facilitate electronic filing of documents with the Government agencies & further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 & the Reserve Bank of India Act, 1934 & for matters connected therewith or incidental thereto.

Objectives of the Act are:

- To grant legal recognition for transactions carried out by means of **electronic data interchange** & 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 & give legal sanction to **electronic fund transfers** between banks & financial institutions
- To give legal recognition for **keeping of books of accounts by banker's** in electronic form.
- To **amend the Indian Penal Code**, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, & the Reserve Bank of India Act, 1934.

Question 3

Define the following with reference to Section 2 of IT (Amendment) Act, 2008:

(i) Adjudicating Authority

Answer

(i) Adjudicating Authority: It means an adjudicating officer appointed under sub-section (1) of Section 46.

Question 4

How does the Information Technology (Amendment) Act 2008 enable the authentication of records using digital signature?

Or

What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature?

Or

How does the information technology act, 2008 enable the authentication of records using digital signatures?

Or

Write short note on Authentication of electronic records in information technology act 2008

Answer

Chapter-ll, Section 3 of Information Technology (Amendment) Act 2008, provides conditions subject to which an electronic record is authenticated by means of affixing digital signature.

- The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record.
  Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

- Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest & which can be verified by anybody who has the corresponding public key.

This will enable anybody to verify whether the electronic record is retained intact or has been tampered with; since it was fixed with the digital signature. It will also enable person who has a public key to identify the originator of the message.

Chapter II of IT act 2008 gives legal recognition to electronic records & digital signature. Section 3 throws light on these conditions.

[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 & hash function which develop & transform the initial record into another electronic record.

Explanation- For the purpose of this section "hash Function" means an algorithm mapping or translation of one sequence of bits into another, generally, smaller, set known as 'Hash Function' 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 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 & the public key are unique to the subscriber & constitute a functioning key pair.

Question 5

How does the Information technology (Amendment) Act 2008 enable the objective of the Government in spreading e-governance?

Answer:

Electronic Governance: It specifies the procedures to be followed for sending & receiving of electronic records & the time & the place of the dispatch & receipt.

Section 4 provides for **"legal recognition of electronic records".** It provides that where any law requires that any information or matter should be in the typewritten or printed

form then such requirement shall be deemed to be satisfied if such information or matter is

a) rendered or made available in an electronic form; &

b) accessible so as to usable for a subsequent reference.

Section 5 provides for **legal recognition of Digital Signatures**. Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the central Government.
For the purpose of this section, "signed", with its grammatical variations & cognate expressions, shall, with reference to a person, mean affixing of his hand written signatures or any mark on any document & the expression "signature" shall be constructed accordingly.

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

Section 7 provides that the document, records or information which is to be **retained for any specified period** shall be deemed to have been retained in the electronic form with the following conditions are satisfied:

(i) The information therein remains accessible so as to be usable subsequently.

(ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.

(iii) The details which will facilitate the identification of the origin, destination, dates & time of dispatch or receipt of such electronic record to be dispatched or received.

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

Moreover this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records, publication of rules, regulations, etc in electronic gazette.

Section 8 provides it provides for the publication of rules, regulations & notifications in the **Electronic Gazette**. It provides that where any law requires the publication of any rule regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form. It also provides where the official Gazette is published both in the

printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

Question 6

Write short note on power of Central Govt. to make rules in respect of Electronic Signature. (Sec 10)

Answer

[Sec. 10] Power to make rules by Central Government in respect of Electronic Signature: The Central Government may, for the purposes of this Act, by rules, prescribe

(a) The **type** of Electronic Signature;

(b) The **manner & format** in which the Electronic Signature shall be affixed;

(c) The manner or procedure which facilitates **identification of the person** affixing the Electronic Signature;

(d) Control processes & procedures to ensure **adequate integrity, security & confidentiality** of electronic records or payments; &

(e) **Any other matter** which is necessary to give legal effect to Electronic Signature.

Question 7

Write short note on Secure Electronic Records & Secure Electronic Signatures

Answer

Secure Electronic Records & Secure Electronic Signatures [Chapter V]

Chapter V sets out the conditions that would apply to qualify electronic records & digital signatures as being secure. It contains sections 14 to 16.

Section 14 provides where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. In ITAA 2008, Section 14 is given as follows:

[Section 14] Secure Electronic Record:

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Section 15 provides for the security procedure to be applied to Digital Signatures for being treated as a secure digital signature. In ITAA 2008, Section 15 is given as under:

[Section 15] Secure Electronic Signature (Substituted vide ITAA 2008):

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

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory & no other person; &
(ii) the signature creation data was stored & affixed in such exclusive manner as may be prescribed

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

Section 16 provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records & secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability & cost of alternative procedures, volume of similar transactions entered into by other parties etc. As per ITAA 2008, Section 16 is given as follows:

[Section 16] Security procedures & Practices (Amended vide ITAA 2008):

The Central Government may for the purposes of sections 14 & 15 prescribe the security procedures & practices.

Provided that in prescribing such security procedures & practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

Question 8

Explain with reference to "Information Technology (Amendment) Act 2008":

(i) Penal Provisions

Answer

(i) Penal Provisions: Chapter IX contains sections 43 to 47. It provides for awarding compensation or damages for certain types of computer frauds. It also provides for the appointment of Adjudication officer for holding an inquiry in relation to certain

computer crimes & for awarding compensation. **Sections 43 to 45 deal with different nature of penalties.**

Penalty for damage to computer, computer system or network:

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

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

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

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

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

(e) Disrupting any computer, computer system or network;

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

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

(h) Charging the services availed of by one person to the account of another person by tampering with or manipulation any computer, computer system or network.

Explanation - For the purpose of this section,-

(i) "**computer contaminant**" means any set of computer instructions that are designed:
   (a) To modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or
   (b) By any means to disrupt the normal operation of the computer, computer system, or computer network;

(ii) "**computer database**" means a representation or information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network & are intended for use in a computer, computer system or computer network;

(iii) "**computer virus**" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the

performance of a computer resource or attaches itself to another computer resource & operates when a program, data or instruction is executed or some other event takes place in that computer resource;

(iv) "**Damage**" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Section 44 states that if any person who is required under this Act or any rules or regulations made there under to:

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

(b) File any return or furnish any information, books or other documents within the time specified in the regulations fails to file, return or furnish the same within the time specified in the regulations, he shall be liable to a penalty not exceeding **five thousand rupees for every day** during which such failure continues;

(c) Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding **ten thousand rupees for every day** during which the failure continues.

Section 45 provides for residuary penalty. Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

The Offences & Penalties under Chapter XI:-

SECTION	OFFENCE	PENALTY
Sec 65	Tampering with computer source documents	• Imprisonment upto **3** years, **or** • Fine upto Rs. 2,00,000, **or** • Both.
Sec 66	Damage to Computer & computer system	• Imprisonment upto **3** years, **or** • Fine upto Rs. 5,00,000, **or** • Both
Sec 66A	Sending offensive messages through computer resource	• Imprisonment upto **3** years, **and** • Fine
Sec 66B	Dishonestly receives stolen computer resource	• Imprisonment upto **3** years, **or** • Fine upto Rs. 1,00,000, **or**

		• Both.
Sec 66C	Identity theft	• Imprisonment upto **3** years, **and** • Fine upto Rs. 1,00,000
Sec 66D	Cheating by personation	• Imprisonment upto **3** years, **and** • Fine upto Rs. 1,00,000
Sec 66E	Violation of Privacy	• Imprisonment upto **3** years, **or** • Fine upto Rs. 2,00,000, **or** • Both.
Sec 66F	Cyber terrorism	• Imprisonment for life.
Sec 67	Publishing & transmitting obscene information in e-form	• First conviction – Imprisonment upto **3** years **and** fine upto Rs. 5,00,000. • Second/ Subsequent conviction - Imprisonment upto **5** years **and** fine upto Rs. 10,00,000.
Sec 67A	Publishing material containing sexually explicit act in e-form	• First conviction – Imprisonment upto **5** years **and** fine upto Rs. 10, 00,000. • Second/ Subsequent conviction - Imprisonment upto **7** years **and** fine upto Rs. 10, 00,000.
Sec 67B	Publishing material depicting children in sexually explicit act in e-form	• First conviction – Imprisonment upto **5** years **and** fine upto Rs. 10,00,000. • Second/ Subsequent conviction - Imprisonment upto **7** years **and** fine upto Rs. 10,00,000.
Sec 67C	Preservation of Information by intermediaries	• Imprisonment upto **3** years, **and** • Fine
Sec 68	Non-compliance with Controller's directions	• Imprisonment upto **2** years, **or** • Fine upto Rs. 1,00,000, **or** • Both.
Sec 69	Failure to assist in information decryption	• Imprisonment upto **7** years, **and** • Fine
Sec 69A	Failure to comply with Central Govt Direction	• Imprisonment upto **7** years, **and** • Fine
Sec 69B	Failure to assist in online access to computer resource	• Imprisonment upto **3** years, **and** • Fine
Sec 70	Securing access to protected system	• Imprisonment upto **10** years, **and** • Fine

Sec 70B	Failure to provide information	• Imprisonment upto **1** years, **or** • Fine upto Rs. 1,00,000, **or** • Both.
Sec 71	Misrepresentation	• Imprisonment upto **2** years, **or** • Fine upto Rs. 1,00,000, **or** • Both.
Sec 72	Breach of confidentiality & privacy	• Imprisonment upto **2** years, **or** • Fine upto Rs. 1,00,000, **or** • Both.
Sec 72A	Disclosure of information in breach of lawful contract	• Imprisonment upto **3** years, **or** • Fine upto Rs. 5,00,000, **or** • Both.
Sec 73	Publishing false ESCs	• Imprisonment upto **2** years, **or** • Fine upto Rs. 1,00,000, **or** • Both.
Sec 74	Publication for fraudulent purpose	• Imprisonment upto **2** years, **or** • Fine upto Rs. 1,00,000, **or** • Both.
Sec 84B	Abatement of Offence	• Punishment provided for the offence under this Act.
Sec 84C	Attempt to commit offence	• Imprisonment of any description provided for the offence, for a term upto one-half of the longest term of imprisonment provided for that offence, **or** • With such fine provided for the offence, **or** • Both

Note:-

1. Provisions of Sec 67, 67A & 67B does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in e-form-

   (a) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

   (b) Which is kept or used for bonafide heritage or religious purposes.

2. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act. **(Sec 78).**

Question: 9

Write short notes on Power of Police Officer & Other Officers to Enter, Search, etc. [Section 80]

Answer

1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place & search & arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act
   Explanation- For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

2. Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

3. The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section

[Section 81] Act to have Overriding effect:

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970 (Inserted Vide ITAA 2008)

Question 10

State the liabilities of companies under section 85 of IT (Amendment) Act, 2008.

Answer

Liability of companies under section 85 of IT (Amendment) Act, 2008: Where a company commits any offence under this Act or any rule there under. Every person who, at the time of the contravention, was in charge of & was responsible for the conduct of the business of the company shall be guilty of the contravention. However, he shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent contravention.

Further, where a contravention has been committed by a company, & it is proved that the contravention took place with the connivance or consent of or due to any negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty & shall be liable to be proceeded against & punished accordingly.

For the purposes of this section, 'company' includes a firm or other association of persons & 'director' in relation to a firm means a partner in the firm.

Question 11

Please read carefully the following three scenarios & answer the question given below:

(a) Scenario 1:
Nobody told you that your Internet use in the office was being monitored. Now you have been warned you will be fired if you use the Internet for recreational surfing again. What are your rights?

(b) Scenario 2:
Your employees are abusing their Internet privileges, but you don't have an Internet usage policy. What do you do?

(c) Scenario 3:
Employee Mr. X downloads adult material to his PC at work, & an employee Miss Y sees it. Miss Y then proceeds to sue the company for sexual harassment. As the employer, are you liable?

Answer

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

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

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

Question 12

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

Answer

Section 6 provides for use of electronic records in government & 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 in Government offices.

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

Question 13

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

Answer

Where any law requires a computer source code to be kept or maintained & any person knowingly or intentionally (whether by himself or through another person), conceals, destroys or alters it, Section 65 provides punishment with imprisonment up to 3 years of fine up to Rs. 2 lakhs, or both

This is to stop persons from hiding or altering computer programs which are required to be maintained under a law. The provision covers only knowing & intentional acts – accidents & mistakes may not be covered.
For the purposes of this section, "Computer Source Code" means the listing of programme, Computer Commands, Design & layout & program analysis of computer resource in any form.

Question 14

Discuss 'Punishment for sending offensive messages through communication service etc.' in the light of Section 66A of Information Technology Act 2000.

Answer

By prescribing imprisonment up to 3 years & fine to person who sends the following, Section 66A protects users of computer systems & communication devices from these:

- **grossly offensive or menacing messages** (e.g. threats to life) ;
- **spam (unsolicited) mails** or messages which cause annoyance, enmity ;
- mails which contain information that the sender knows is **false ;**
- **'Phishing' mails** which try to deceive or mislead the receiver into thinking that the mail was sent by someone else.

Since communication devices are covered, SMS through mobile may also be covered. Contents in attachments to messages are also covered. Contents may be in the form of text, image, audio, video or other form.

Question 15

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

Answer

Certifying Authorities create digital signatures & provide them to subscribers. People use & 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 & 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 16

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) 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, the reasons should be recorded in writing,

(2) The Procedure & 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 & 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 & fine.

Question 17

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

Answer

Digital signatures are very important for electronic commerce & Section 73 provides strong controls to prevent their misuse. It provides imprisonment up to 2 years, fine up to Rs. 1 lakh, or both for knowingly publishing or making available an electronic signature certificate:

- Which is not issued by the Certifying authority listed in it ; or
- The subscriber has not issued it ; or
- The certificate is revoked or suspended

However, it could be published for verifying a digital signature created before the certificate was suspended or revoked.

Question 18

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 & resilient cyberspace for citizens, business & Government" & the mission "To protect information & information infrastructure in cyberspace, build capabilities to prevent & respond to

cyber threats, reduce vulnerabilities & minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology & cooperation".

Major objectives of this policy are given as follows:

- **Secure cyber ecosystem**: To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems & transactions in cyberspace & thereby enhance adoption of IT in all sectors of the economy;
- **Compliance to global security standards:** To create an assurance framework for design of security policies & for promotion & enabling actions for compliance to global security standards & best practices by way of conformity assessment (product, process, technology, & people);
- **Strengthening the regulatory framework:** To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem;
- **National & sectorial level mechanism 24/7:** To enhance & create National & Sectorial level 24*7 mechanisms for obtaining strategic information regarding threats of ICT infrastructure creating scenarios for response, resolution & crisis management through effective predicative, protective, response & recovery actions;
- **24*7 (NCIIPC):** To enhance the protection & resilience of Nation's critical information infrastructure by operating a 24*7 National Critical Information Infrastructure Protection Center(NCIIPC) & mandating security practices related to the design, acquisition, development & operation of information resources;
- **Developing suitable indigenous technology:** To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, & pilot development of secure ICT products/processes in general & specifically for addressing National Security requirements;
- **Better integrated ICT products:** To improve visibility of the integrity of ICT products & services & establishing infrastructure for testing & validation of security of such products;
- **Create Professional workforce:** To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development & training;
- **Fiscal Benefits**: To provide fiscal benefits to businesses for adoption of standard security practices & processes;

- **Protection of Information:** To enable protection of information while in process, handling, storage & transit so as to Safeguard privacy of citizen's data & for reducing economic losses due to cyber crime or data theft;

- **Investigation & prosecution of cybercrimes:** To enable effective prevention, investigation & prosecution of cybercrime & enhancements of law enforcement capabilities through appropriate legislative intervention;

- **Creating a culture of cyber security:** |: To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication & promotion strategy;

- **Public private partnership:** To develop effective public private partnerships & collaborative engagements through technical and operational collaboration & contribution for enhancing the security of cyberspace &

- **Global Cooperation:** To enhance global cooperation by promoting shared understanding & leveraging relationships for furthering the cause of security of cyberspace.

Requirements of Various Authorities for System Controls & Audit

In this section, we will discuss controls & audit requirements by various statutory bodies such as IRDA, RBI & SEBI.

Please note that the descriptions covered in ISCA are just illustrative & comprehensive:

Question 19

IRDA Requirements for System Controls & Audit

The Insurance Regulatory & Development Authority of India (IRDA) is the apex body overseeing the insurance business in India. It protects the interests of the insurance policyholders. It regulates. Promotes & ensures orderly growth of the insurance business in India.

(i) System audit requirements: The requirements for this audit are as follows:

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

(ii) Preliminaries: Before starting IS audit, an auditor needs to understand the following:

- Location(s) from where insurance company's investment activity is conducted.
- IT applicants/software used to manage the company investment portfolio.
- Information about IT System & network infrastructure including: Server details, database details, type of network connectivity, firewalls other facilities/ utilities (describe).
- Review IT security policy, Business Continuity Plans & IT network security reports etc.
- Check whether systems & applications hosted at a central location or hosted at different offices?
- Review previous audit reports such as: Statutory Audit, Internal Audit & IRDA inspection/audit reports for any open issues etc.
- Review of internal circulars & guidelines for Insurer
- Review of IRDA notifications, circulars & correspondences
- Review of SOP (Standard Operating Procedures) for insurance companies
- Review list of new products/funds introduced during this audit period & review of investment as per IRDA guidelines

(iii) System Controls: Auditor can verify the following controls:

- Verify that audit trail exists for every transaction in system.
- Verify that all systems within the organizations & inter organization are integrated & data is transferred electronically between systems without manual intervention
- The auditor review the insurance company's software/Investment management system for FOS (Front Office Module), MOS (Mid Office Module) & BOS (Back Office Module) & confirm that the system maintains audit trail for data entry, authorization, cancellation & any subsequent modifications.
- Further, the auditor shall also verify that the system has separate logins for each user & maintains trail of every transactions with respect to login ID, date & time for each data entry, authorization & modification.

RBI requirements for System Controls & Audit

The Reserve Bank of India (RBI) is India's central banking institution. RBI formulates the monetary policies with regard to the Indian economy & banking system.

The RBI was constituted to meet the following needs for India:

- Regulate banking organizations & issues new banking license
- Regulate & the issue of banknotes,

- Maintain reserves with a view to securing monetary stability, & operate the credit & currency system of the country to its advantage.

The banking organizations are the most automated & biggest users of IT systems. RBI has been proactive in providing guidelines to implement IT systems with the best global practices. RBI also has various committees who review existing & futures banking related technologies & risks & providing guidelines accordingly.
IS audit has become very important for banking organizations as key processes are automated & RBI has been providing guidelines for IS audit financial institutions.
RBI & senior management of banks need assurance that internal controls implemented for banking systems are effective & adequate. For this, RBI & management rely on IS audit to provide an independent view on implemented internal controls & need assurance that the IT related risks are managed.

This IS Audit assignments covers the following.

(i) System Controls: The following provide effective system controls for banking organizations

- Board of directors & senior management are responsible for effective IT system controls
- There is an IS audit policy & this is reviewed for effectiveness annually
- Bank conducts once in a three year quality assurance for IS audit to validate the approach & practices adopted in IS audit are as per IS audit policy
- Bank uses appropriate control measures to protect computer system from the attacks of unscrupulous elements
- Formal methods/standards are there for change of software across bank's branches /offices to maintain a uniformity of applications across banks.
- There should be segregation of duties i.e. programmer who designed & developed the system should not be given responsibilities of operating the system. Similarly person responsible for maintenance of system should be different than persons who designed /developed & operating the system.

(ii) System Audit: IS Audit has become important function in the banking organization due to over reliance of banking organizations on IT system for day-to-day working. The following should be part of IS Audit in the banking organizations:

- IS Audit should be separate function within an Internal Audit department led by IS audit head & reporting to Head of Internal Audit or CAE (Chief Audit Executive)

- Bank can leverage external help for IS audit with responsibility/accountability with IS Audit head & CEA for getting this audit done.

- Auditors need to be independent & competent professional for IS Audit

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

- **Auditors' Competence:** IS Auditors should be professionally competent, having skills, knowledge, training & relevant experience with professional certifications in IS Audit. As IT consists of a wide range of technologies, IS Auditors should possess skills that are in line with the technologies used by banks. Qualifications such as CISA (offered by ISACA), DISA (offered by ICAI), or CISSP (offered by ISC^2), along with two or more years of IS Audit experience, are desirable. Similar qualification criteria should also be insisted upon, in case of outsourced professional service providers.

  The following should be subjected to IS audit at-least once a year:
  - IT Governance
  - IT Security
  - Critical applications/system
  - Data centers controls & processes
  - Regulatory compliance requirements
  - Branches with focus on large & medium branches in areas such as:
    - Password controls
    - Operating system security
    - Protection from virus/malware/destructive programs
    - Physical security
    - Audit trail
    - Segregation of duties
    - BCP, etc

  - Controls for new system development including all phases of SDLC
  - Post implementation review of application controls
  - Application controls for correct processing, inputs & outputs
  - Database controls
  - IT related risks & their impacts on banking organization. When IS Auditors believe that the bank has accepted a level of residual risk that is inappropriate for the organization, they should discuss the matter with appropriate level of management. If the IS Auditors are not in agreement with the decision, regarding residual risk, IS Auditors & Senior Management should report the matter to the Board (or Audit Committee) for resolution.

RBI has an inspection wing, which does inspection of banking & non-banking financial institutions. If IS audit has not been done, it is considered as non-compliance. It should be reported to the senior management for compliance. In the case of branch statutory

audit, the LFAR (Long Form Audit Report) has specific questions pertaining to IT areas such as Security/BCP etc., which need to be reviewed by the statutory auditors. These can also be considered as key areas of IS Audit.

Requirements of SEBI for System Controls & Audit

The Securities & Exchange Board of India (SEBI) is the regulator for the securities market in India. SEBI is responsible for managing needs of following:

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

(i) Systems Audit:

- SEBI has 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) & Guidelines issued by SEBI.
- Stock Exchange/Depository (Auditee) may negotiate & the board of Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms & 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 & 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 & cover any open items therein.
- The management provides their comment about the Non-Conformities (NCs) & observations.
- For each NC, specific time-bound (within 3 months) corrective action must be taken & reported to SEBI. The auditor should indicate if a follow-on audit is required to review the status of NCs. The report along with Management
- Comments shall be submitted to SEBI within 1 month of completion of the audit. Sample areas of review covered by IS Audit assignments are given here.

(ii) Audit Report Norms: These includes the following

- The systems Audit Reports & Compliance Status should be placed before the Governing Board of the Stock Exchanges/Depositories & the system audit report

along with comments of Stock Exchanges/ Depositories should be communicated to SEBI.

- The Audit report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or Observations (or lack of it).
- For each section, auditors should also provide qualitative input about ways to improve the process, based upon the best practices observed.

(iii) Auditor Selection Norms: Auditor selection norms include the following:

- 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 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 Security Manager) from ISACA, GSNA (GIAC Systems & 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 & processes conforming to industry leading practices like CoBIT.
- The Auditor must not have any conflict of interest in conducting fair, objective & independent audit of the Exchange/Depository. It should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
- The Auditor may not have any cases pending in its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence &/or unsuitability to perform the audit task.

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

- Further, along with the audit report, Stock Exchanges/Depositories are advised to submit a declaration from the MD/CEO certifying the security & integrity of their IT Systems.
- A proper audit trail for upload/modifications/downloads of KYC data to be maintained.

Department of Electronics & IT, Ministry of Communication & IT, Government of India, maintains a panel of systems auditors, who are used by Government enterprises for system audit. This provides information on scope of different types of systems audit which is used as reference by audit firms for getting systems audit done.

Question 20

Write short notes on Cyber Forensic & Cyber Fraud Investigation

Answer:

- Cyber Forensic is related with **investigation of internet/computer related frauds.**
- Cyber Forensic is one of the **latest scientific techniques** & it has emerged due to increasing internet/computer frauds.
- Here **Cyber means internet world** or computer/digital systems & forensics is a scientific method of investigation. It includes analysis techniques to gather, process, interpret, & to use evidence to provide a conclusive description of activities in a way that it is suitable for presentation in the court of law.
- 'Cyber' & 'Investigation' together **is an investigation method gathering digital evidences** to be produce in court of law.
- Court rulings & cyber laws now **permit courts to rely upon digital evidences.**
- In Cyber Forensic, **electronic evidences** are created by **using scientific techniques.**
- Cyber Forensic emphasis the use of **special methods to gather evidences**, so that these electronic evidences stand the scrutiny when **presented in the court of law.**
- Cyber Forensic experts follow **standard methods for investigation**. The experts of the fields use standard processes & globally accepted methods so that same result shall always be obtained if the same evidences are checked by another expert.
- There is significant increase of frauds across the cyber space & fraudsters are always on the look-out to **misuse any loop hole or weaknesses in the computer systems.**
- Cyber Frauds have increased across the world as fraudulent transfer/withdrawal of amount **using net banking & using ATM cards** run into 100s of millions of dollars & have created a big challenge for IT security agencies.
- There is an increasing demand for experts in the field of Cyber Forensics.

The IT Act under section 43A & Section 65 to 67B lists various types of cyber crimes & specifies penalty for them. For example, section 65, which have already been discussed in earlier sections. Keeping importance of this, the Institute of Chartered Accountants of India, New Delhi, has also launched a post qualification course on the above subject by the name "Certificate Course on Forensic Accounting & Fraud Detection." This post qualification course can be taken by a qualified CA.

Question 21

Write short notes on Information Security Standards & National Cyber Security Policy 2013

Answer:

Information Security has become very important function of organization due to increasing threats from hackers, computer crimes, virus, etc. Breaches in information security can lead to a substantial impact for organization in terms of financial or operational damages. In addition, the enterprise can be exposed to reputational & legal risks which can spoil relationship between organization & customer/employee & even put the organizational survival in danger.
COBIT 5 for information security published by ISACA & ISO 27001 highlights the needs for information security in organization & provide standards for implementing information security. COBIT 5 & ISO27001 help for the following:

- Maintain information risk at an acceptable level
- Protect information against unauthorized disclosure, unauthorized or accidental modifications & protect instructions.
- Ensure that services & systems are continuously available to internal & external users, leading to user satisfaction with IT system & services
- Comply with the growing number of relevant laws & regulations as well as contractual requirements & internal policies on information & systems.
- Provide transparency on the level of compliance & achieve all the while containing the cost of IT services & technology protection.

ISO 27001- INFORMATION SECURITY MANAGEMENT STANDARD

1) ISO 27001 is the international best practice & standard for information Security Management System (ISMS). An ISMS is a systematic approach to managing confidential or sensitive information so that it remain secure (which means available, confidential & with its integrity intact). It encompasses people, processes & IT systems.

2) Information Security is not just about anti-virus software, implementing the latest firewall or locking down the laptops or web servers. The overall approach to information security should be strategic as well as operational, & different security initiatives should be prioritized, Integrated & cross-referenced to ensure overall

effectiveness. An ISMS helps us coordinate all our security efforts-both electronic & physical- coherently, consistently & cost effectively.

3) ISO 27001 defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large. It is safe to say that standard is the foundation of information security management. ISO 27001 is for information security. It is a standard written by the world's best experts in the field of information security in an organization. It also enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the best possible way in the organization.

FOUR PHASES OF ISMS: -

ISO 27001 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.

The detail description of these phases is as follows:-

1) **THE PLAN PHASE**:- This phase serves to plan the basic organization of information security, set objectives for information security & choose the appropriate security controls. It consists of the following steps:-

   a) Determining the scope of the ISMS
   b) Writing an ISMS policy
   c) Identifying the methodology for risk assessment & determining the criteria for risk acceptance;
   d) Identification of assets, vulnerabilities & threats;
   e) Evaluating the size of risk;
   f) Identification & assessment of risk treatment options;
   g) Selection of controls for risk treatment;
   h) Obtaining management approval for residual risks;
   i) Obtaining management approval for implementation of the ISMS; &
   j) Writing a statement of applicability that lists all applicable controls, state which of them already been implemented & those which are applicable.

2) **THE DO PHASE**:- this phase includes carrying out everything that was planned during the previous phase. This phase consists the following steps:-
   a) Writing a risk treatment plan- describes who, how when & with what budget applicable controls should be implemented.
   b) Implementing the risk treatment plan;
   c) Implementing applicable security controls;
   d) Determining how to measure the effectiveness of controls;
   e) Carrying out awareness programs & training of employees;
   f) Management of the normal operation of the ISMS;
   g) Management of ISMS resources; &
   h) Implementation of procedures for detecting & managing incidents.

3) **THE CHECK PHASE**:- The purpose of this phase is to monitor the functioning of the ISMS through various channels, & check whether the result meet the set objectives:- This phase includes the following:-

   a) Implementation of procedures & other controls for monitoring & reviewing in order to establish any violation, incorrect data processing, whether the security activities are carried out as expected, etc:
   b) Regular reviews of the effectiveness of the ISMS;
   c) Measuring the effectiveness of controls;
   d) Reviewing risk assessment at regular intervals;
   e) Internal audits at planned intervals;
   f) Management reviews to ensure that the ISMS is functioning & to identify opportunities for improvement;
   g) Updating security plans in order to take account of other monitoring & reviewing activities &
   h) Keeping records of activities & incidents that may affect the effectiveness of the ISMS

4) **THE ACT PHASE**:-The purpose of this phase is to improve everything that was identified as non- compliant in the previous phase; This phase includes the following-

   a) Implementation of identified improvements in the ISMS;
   b) Taking corrective & preventive action; Apply own & others security experience;
   c) Communicating activities & improvements to all stakeholders &
   d) Ensuring the Improvements achieve the desired objectives.

ITIL (IT INFRASTRUCTURE LIBRARY)

1) The Information Technology Library (ITIL) is a set of practices of IT service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage.

2) ITIL describes procedures, tasks & checklists that are not organization specific, 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 & measure. IT is used to demonstrate compliance & to measure improvement.

3) Although the UK government originally created the ITIL, it has rapidly been adopted across the world as the standard for best practices in the provision of information technology services. ITIL assists in establishing a business management approach & discipline to IT service management, stressing the complementary aspects of running IT like a business.

4) ITIL V3 represents an important change in best practice approach, transforming ITIL form proving a good service to being the most innovative & best in class. It also brought a rationalization in the number of volumes included in the set which now comprises the following:-
   a) Service Strategy
   b) Service Design
   c) Service Transition
   d) Service Operation, &
   e) Continual Service Improvement.

DETAILS OF THE ITIL FRAMEWORK-

1) **Service Strategy**: Service strategy deals with the strategic management approach in respect of IT service management; strategic analysis; planning positioning, & implementation relating to service models, strategies & strategic objectives. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers.

2) **Service Design:-** Service design translates strategic plans & objectives & creates the design & specification for execution through service transition & operations. It provides guidance on combining infrastructure, application, systems and processes, along with suppliers and partners, to present feasible service offerings.

3) **Service transition**:- Service transition provides guidance on the service design & implementation, ensuring that the service delivers the intended strategy & that it can be operated and maintained effectively.

4) **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 & architecture such as shared services, utility computing, web services and mobile commerce.

5) **Continual Service improvement:-** It provides guidance on the measurement of service performance through the service life-cycle, suggesting improvements to ensure that a service delivers the maximum benefit. This volume provides guidance on creating & maintaining value for customers through improved design, introduction, and operation of services. It combines principles, practices & methods from change management, quality management, in service quality, operational efficiency and business continuity.

Chapter-8

EMERGING TECHNOLOGIES

Question 1

What is Cloud Computing? Explain some pertinent similarities and differences between Cloud and Grid computing.

Answer

Cloud Computing:

It is a network technique which helps organisations to share resources using internet. A cloud is collection of servers, applications, database, documents, agreements, spreadsheets, storage capacity etc which allows organisations to share these resources from anywhere.

Cloud computing is the delivery of computing services over the internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties like Google, Microsoft, Amazon, IBM etc at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business application. The cloud computing model allows access to information and computer resources from anywhere using internet. Cloud Computing provides a shared pool of resources, including data storage space, networks, computer processing power and specialized corporate and user application.

Cloud computing simply means the use of computing resources as a service through networks, typically the Internet. With Cloud Computing, users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.

Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service. With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software.

In Cloud Computing:

- The consumer or user no longer has to be at a PC i.e. user can use any device for using applications.
- The consumer does not purchase a specific version of software which is required to be configured for smartphones; PDA's and other devices i.e. can download the required version from cloud.
- The consumer or end user does not own the infrastructure, software or platform in the cloud, this leads to lower upfront costs or capital expenses.

- The consumer or user does not care about how servers and networks are maintained in the cloud.

- The consumer can access multiple servers from anywhere on the globe without knowing where they are located.

GRID Computing

- Imagine several million computers from all over the world, and owned by thousands of different people. Imagine they include desktops, laptops, supercomputers, data vaults, and instruments like mobile phones, meteorological sensors and telescopes...

  Now imagine that all of these computers can be connected to form a single, huge and super-powerful computer! This huge, sprawling, global computer is what many people dream "The Grid" will be.

  "The Grid" takes its name from an analogy with the electrical "power grid". The idea was that accessing computer power from a computer grid would be as simple as accessing electrical power from an electrical grid".

Some pertinent similarities and differences between cloud and grid computing are highlighted as follows:

Similarities:

- **Scalable:** Cloud computing and grid computing both are scalable. Scalability is accomplished through load balancing of application instances running separately on a variety of operating systems and connected through Web services. CPU and network bandwidth is allocated and de-allocated on demand. The system's storage capacity goes up and down depending on the number of users, instances, and the amount of data transferred at a given time.

- **Multi- tenancy and multitasking:** Both computing types involve multi-tenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances. Sharing resources among a large pool of users assists in reducing infrastructure costs and peak load capacity.

- **High uptime availability:** Cloud and grid computing provide Service-Level Agreements (SLAs) for guaranteed uptime availability of, say, 99 percent. If the service slides below the level of the guaranteed uptime service, the consumer will get service credit for not receiving data within stipulated time.

Difference:

- **Data storage:** While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.

- **Computations:** A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

Question 2

Discuss the major goals of Cloud computing in brief.

Answer

Major goals of cloud computing are given as follows:

- **Highly efficient Ecosystem:** To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;
- **Anywhere anytime access:** To access services and data from anywhere at any time;
- **Quick Scalability:** To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;
- **Consolidation:** To consolidate IT infrastructure into a more integrated and manageable environment;
- **Reduced cost:** To reduce costs related to IT energy/power consumption;
- **Anywhere access:** To enable or improve "Anywhere Access" (AA) for ever increasing users; and
- **Provision of resources:** To enable rapid provision of resources as needed.

Question 3

Describe Front end and Back end architecture with reference to Cloud Computing.

Answer

Front End Architecture: The front end of the cloud computing system comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users.

Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.

Back End Architecture: Back end refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system.

Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment.

Usually, every application would have its individual dedicated server for services.

In addition, a central server is established which is used for administering the whole cloud system. It is also used for monitoring client's demand as well as traffic to ensure that everything of system runs without any problem. There are some set of rules, generally called as protocols which are followed by this server and it uses a very special type of software known as middleware. Middleware allows computers that are connected on network to make communication with each other. Also a backup and recovery system of data is maintained for security purpose.

Question 4

What do you understand by Public cloud? Also discuss its major advantages in brief.

Answer

Public Clouds: This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis.

These are also called provider clouds. Business models like SaaS (Software-as-a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services.

The Advantages of public cloud include the following:

- **Development, Deployment:** It is widely used in the development, deployment and management of enterprise applications, **at affordable costs.**

- **Scalable and reliable**: It allows the organizations to deliver highly scalable and reliable applications rapidly and **at more affordable costs.**

Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen.

Question 5

What is Private cloud? Also explain its major advantages in brief.

Answer

Private Clouds: This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

The advantages of private clouds include the following:

- **Higher efficiency:** They improve average server utilization; allow usage **of low-cost** servers and hardware while providing higher efficiencies; thus reducing the costs that a greater number of servers would otherwise entail.

- **Automation:** High levels of automation is largely responsible for **reducing operations costs** and administrative overheads

However, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently.

Question 6

Explain the following with reference to cloud computing:

(a) Infrastructure as a Service (IaaS),
(b) Platform as a Service (PaaS),
(c) Software as a Service (SaaS),
(d) Network as a Service (NaaS), and
(e) Communication as a Service (CaaS).

Answer

Cloud Computing providers offer their services according to several fundamental models. These are known as cloud computing service models.

(a) **Infrastructure as a Service (IaaS):** IaaS providers offer computers, more often virtual machines and other resources as service. It provides the infrastructure / storage required to host the services by ourselves i.e. makes us the system administrator and manage hardware/storage, network and computing resources. In order to deploy their applications, cloud clients install operating-system images and their application software on the cloud infrastructure. Examples of IaaS providers include: Amazon EC2, Azure Services Platform, Dyn DNS, Google Compute Engine, HP Cloud etc.

(b) **Platform as a Service (PaaS):** Cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of acquiring and managing the underlying hardware /software layers. In PaaS, one can make applications and software on other's database. Thus, it gives us the platform to create, edit, run and manage the application programs we want. All the development tools are provided. Some of examples of PAAS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard etc.

(c) **Software as a Service (SaaS):** SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. For example, one can make his/her own word document in Google docs online, she can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system- thus Google is provisioning software as a service.

(d) **Network as a Service (NaaS):** It is a category of cloud services where the capability provided to the cloud service user is to use network/transport connecting services. NaaS involves optimization of resource allocation by considering network and computing resources as a whole. Some of the examples are: Virtual Private Network, Mobile Network Virtualization etc.

(e) **Communication as a Service (CaaS):** CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vendor. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates large capital investments. Examples are: Voice over IP (VoIP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.

Question 7

Explain, in brief, the characteristics of Cloud Computing.

Answer

Major characteristics of cloud computing is given as follows:

- **High Scalability:** Cloud environments enable servicing of business requirements for larger audiences, through high scalability.
- **Agility:** The cloud works in the 'distributed mode' environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness).
- **High Availability and Reliability:** Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
- **Multi-sharing:** With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
- **Services in Pay-Per-Use Mode:** SLAs between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.
- **Virtualization:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
- **Performance:** It is monitored and consistent and its loosely coupled architecture constructed using web services as the system interface enables high level of performance.
- **Maintenance:** The cloud computing applications are easier, because they are not to be installed on each user's computer and can be accessed from different places.

Question 8

Briefly discuss the advantages of Cloud Computing.

Answer

Major advantages of Cloud Computing are given as follows:

- **Cost Efficiency:** Cloud computing is probably the most cost efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot in terms

of finance. Adding up the licensing fees for multiple users can prove to be very expensive for the establishment concerned. The cloud, on the other hand, is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.

- **Almost Unlimited Storage:** Storing information in the cloud gives us almost unlimited storage capacity. Hence, one no more need to worry about running out of storage space or increasing the current storage space availability.

- **Backup and Recovery:** Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

- **Automatic Software Integration:** In the cloud, software integration is usually something that occurs automatically. This means that we do not need to take additional efforts to customize and integrate the applications as per our preferences. This aspect usually takes care of itself. Not only that, cloud computing allows us to customize the options with great ease. Hence, one can handpick just those services and software applications that s/he thinks will best suit his/her particular enterprise.

- **Easy Access to Information:** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.

- **Quick Deployment:** Lastly and most importantly, cloud computing gives us the advantage of quick deployment. Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes. Of course, the amount of time taken here will depend on the exact kind of technology that we need for our business.

Question 9

Explain some of the tangible benefits of mobile computing.

Answer

Major tangible benefits of mobile computing are given as follows:

- It provides **mobile workforce (field staff) with remote access to work** order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.

- It enables mobile sales personnel to **update work order** status in real-time, facilitating excellent communication.

- It facilitates access to **corporate services and information at any time, from anywhere.**

- It provides **remote access** to **the corporate Knowledgebase** at the job location.

- It enables us to **improve management effectiveness** by enhancing information quality, information flow, and ability to control a mobile workforce.

Question 10

Write short notes on the following:

(i) Hybrid Cloud
(ii) Mobile Computing
(iii) BYOD
(iv) Web 2.0
(v) Green IT

Answer:

(i) Hybrid Cloud: This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

(ii) Mobile Computing: It is like mobile phone service. This provides ability to use computing capability without a pre-defined location and connection to a particular network to publish and access information. Mobile computing is considered an extension of mobile phone service. It is related to transfer and receipt of data over the cellular phone network.

Mobile computing allows using data and data processing services from anywhere while on move i.e. while moving from one location to another. There are many popular mobile computing devices.

- Personal digital assistant/enterprise digital assistant.
- Smartphone
- Tablet computer
- Ultra-mobile PC

It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution of the biggest problem of business people on the move i.e. mobility.

(iii) BYOD: BYOD (**B**ring **Y**our **O**wn **D**evice) refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops, challenging the long-standing policy of working on company-owned devices. Though it has led to an increase in employees' satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

The BYOD Policy has allowed the employees to be mobile and gives them the right to work beyond their required hours. The new technology has led to mass adoption of smart phones, tablets and laptops and it is challenging the traditional policy of working on company owned devices only. Renowned research organisation "Gartner" has predicted that by 2014, 90% of organisations will support corporate application on personal devices.

(iv) Web 2.0: Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability of people to collaborate and share information online. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information. Over the time, Web 2.0 has been used more as a marketing term than a Computer Science based term. Blogs, wikis, and Web services are all seen as components of Web 2.0. Web 2.0 tries to tap the power of humans connected electronically through its new ways at looking at social collaboration. The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner. In this regard, many new concepts have been created such as Blogging, Social Networking, Communities, Mash-ups, and Tagging. The power of Web 2.0 is the creation of new relationships between collaborators and information.

(v) Green IT: Green IT refers to the study and practice of establishing / using computers and IT resources in a more efficient, environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle. It is largely taken as the study and practice of designing, manufacturing, using, and disposing of computers, servers, associated subsystems and peripheral devices efficiently and effectively with highly mitigated negative impact on the environment. The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Many corporate IT departments have Green Computing initiatives to reduce the environmental impacts of their IT operations and things are evolving slowly but not as a revolutionary phenomenon.

Question 11

'The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment'. Discuss some of such steps, which can be followed for Green IT.

Answer

Major steps, which can be followed for Green IT, are given as follows:

- **Power-down the CPU** and all peripherals during extended periods of inactivity.
- Try to do **computer-related tasks during contiguous, intensive** blocks of time, switching off hardware at other times.
- **Power-up and power-down** energy-intensive peripherals such as laser printers according to need.
- **Use Liquid Crystal Display** (**LED/LCD**) monitors rather than Cathode Ray Tube (CRT) monitors.
- **Use notebook computers** rather than desktop computers whenever possible.
- Use the power-management features to turn off **hard drives and displays after several minutes of inactivity**.
- Minimize the **use of paper and properly recycle** waste paper.
- **Dispose of e-waste according to central**, state and local regulations.
- Employ alternative energy sources for computing workstations, servers, networks and data centres.

Question 12

What are the various issues with cloud computing?

Answer

Just like any other technology, before its progress to stabilization and maturity, cloud computing also has several issues. Some of the well-identified issues stand out with cloud computing is described briefly as follows:

- **Threshold Policy**: This is a policy which defines cyclical use of any application e.g. use of credit card will rise sharply during the festival seasons and use will decrease significantly after the festival or buying crunch is over. The program processing the credit card should be having the capability to provide more instances or processing capabilities during buying seasons and deallocate these instances for other work when buying season is over. In order to test if the program works, develop, or improve and implement, a threshold policy is of immense importance in a pilot study before moving the program to the production environment. Checking how the policy enables to detect sudden increases in the demand and results in the creation of additional instances to fill in the demand. Moreover, to determine how unused resources are to be de-allocated and turned over to other work needs to work out in the context. That is working out thresholds is really a matter of concern and would go a long way to assure the effectiveness.

- **Interoperability:** If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary APIs and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. We may need to reformat/reorganize data or change the logic in applications. Although industry cloud-computing standards do not exist for APIs or data import/export, IBM and Amazon Web Services have worked together to make interoperability happen.

- **Hidden Costs:** Like any such services in prevailing business systems, cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges from their service providers for storage and database applications containing terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. In another instance of incurring network costs, companies, who are far from the location of cloud providers, could experience latency, particularly when there is heavy traffic.

- **Unexpected Behaviour:** Let's suppose that credit card validation application works well at our company's internal data centre. It is important to test the application in the cloud with a pilot study to check for unexpected behaviour. Examples of tests include how the application validates credit cards, and how, in the scenario of the buying crunch, it allocates resources and releases unused resources, turning them over to other work. If the tests show unexpected results of credit card validation or releasing unused resources, we will need to fix the problem before executing or obtaining cloud services from the cloud.

- **Security Issues:** Security is a major issue relating to cloud computing. Instead of waiting for an outage to occur, consumers should do security testing on their own checking how well a vendor can recover data. Apart from the common testing practices, what one needs primarily to do is to ask for old stored data and check how long it takes for the vendor to recover. If it takes too long to recover, ask the vendor why and how much service credit we would get in different scenarios. Moreover, in such cases, verifying the checksums match with the original data is a requisite.

  Another area of security testing is to test a trusted algorithm to encrypt the data on the local computer, and then try to access data on a remote server in the cloud using the decryption keys. If we can't read the data once we have accessed it, the decryption keys are corrupted, or the vendor is using its own encryption algorithm. We may need to address the algorithm with the vendor. Another issue is the potential for problems with data in the cloud. To protect the data, one may want to manage his/her own private keys. Checking with the vendor on the private key management is no longer a simple as it appears so.

Question 13

What are the various Challenges relating to Cloud Computing?

Answer

In spite of its many benefits, as mentioned above, cloud computing also has certain challenges. Businesses, especially smaller ones, need to be aware of the same before adapting this technology.

- **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential from the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control).

- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be insured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage.

- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete from Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability. One of the major Cloud service provider, AWS had a breakdown for several hours, which lead to data loss and access issues with multiple Web 2.0 services.

- **Governance:** Due to the lack of control over the employees and services, it creates problem relating to design, implementation, testing and deployment. So there is a need of governance model, which controls the standards, procedures and policies of the organization. The organization gains computational resources as capital expenditures. These actions should be looked by the organization under governance through legal regulation policies, privacy and security. Auditing and risk management programs are some way to verify the policy, which can shift the risk landscape.

- **Trust:** Deployment model provide a trust to the Cloud environment. An organization has direct control over security aspects as well as the federal agencies even have responsibility to protect the information system from the risk. Trust is an important issue in Cloud. Various clients' oriented studies reveal that Cloud has still failed to build trust between the client and service provider. Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.

- **Legal Issues and Compliance:** There are various requirements relating to legal, privacy and data security laws that need to be studied in Cloud system. One of the major troubles with laws is that they vary from place to place, and users have no assurance of where the data is located physically.

  There is a need to understand various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy data location and security controls records management, and E-discovery requirements.

  An approach to monitor and compliance that helps to prepare Cloud Service Provider (CSP) and users to address emerging requirements and the evolution of Cloud models. To achieve efficiency, risk management, and compliance, CSPs need to implement an internal control monitoring function coupled with external audit process. To increase the comfort of Cloud activities, Cloud user define control requirements, internal control monitoring processes, examine applicable external audit reports, and accomplish their responsibilities as CSP users. It is the responsibility of the cloud suppliers that they are protecting the data and supplying to the customer in a very secure and legal way.

- **Privacy:** Privacy is also considered as one of the important issues in Cloud. The privacy issues are embedded in each phase of the Cloud design. It should include both the legal compliance and trusting maturity. The Cloud should be designed in such a way that it decreases the privacy risk.

- **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'. Cloud application security should be stronger than the one built in organisation individual software and application. Audit of cloud computing model is always a challenge as this requires understanding and implementing virtualisation.

- **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing. Some of the Cloud providers do not use their own server, instead. They use server/s from other service providers. In that case, there is a probability that the data is less secure and is more prone to the loss from external server. If the external server is shut down due to any legal problem, financial crisis, natural disaster, and fire creates loss for the user. In that case, data protection is an important mechanism to secure the data. Back up policies such as Continuous Data Protection (CDP) should be implemented in order to avoid issues with data recovery in case of a sudden attack.

- **Architecture:** Security and privacy of data also depends upon architecture of cloud computing service model. In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model. Its reliable and scalable infrastructure is dependent on the design and implementation to support the overall framework.

- **Identity Management and Access control:** Every organisation normally uses its own rules for identity management and access controls (i.e. user id, password and authorization rules) Extending these rules to cloud which is resource of cloud service provider becomes an issue. Because cloud service provider would like to use their own rules of identity management and access controls.

- **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Affected network measures, determined systems, and applications, exposed intrusion vector helps to understand an incident response and the activities carried out must be re-modelled.

- **Software Isolation:** In cloud computing, same software or application is used by different organisation or users. Thus software isolation to protect users from each other is also an issue.

- **Application Security:** In cloud computing, the applications (i.e. software) for data processing are stored on cloud thus face the issues of application security because cloud is accessible by large number of users.

Question 14

What are the various risks associated with Emerging BYOD?

Answer

Every business decision is accompanied with a set of threats and so is BYOD program too; it is not immune from them. As outlined in the Gartner survey, a BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises. Overall, these risks can be classified into four areas as outlined below:

- **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the

network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.

- **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.

- **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.

- **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. It's important that the organisation should have a strong BYOD policy. This policy should be effectively implemented as well. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above mentioned threats. Any weakness in this implementation may result in big loss to organisation.

Question 15

Write short notes on Social Media.

Answer:

We all are part of one or other social networks these days. We are connected with our friends, relatives, by using one or other form of social media or network.

Social media refers to the means of interaction among people in which they create, share, and/or exchange information and ideas in virtual communities and networks.

While considering a network, we imagine a set of entities connected with each other on a logical or a physical basis. Physical networks like computer networks are those that can be planned, implemented and managed very optimally and efficiently. However, when we move from physical to logical networks, the visualization becomes much more difficult. Social networks are comprised of the most intelligent components- human beings. Being so, any activity involved with the social networks, be it participation, management, or optimization becomes extremely complicated and context based. Due to the various facets of the human species, we can have multiple types of social networks in all the fields and areas. This can range from a network of researchers, to a network of doctors to a network of academics. Each type of network has its own focus area, member size, geographical spread, societal impact and objective. Managing such networks is not only complicated but requires lot of collective efforts and collaboration. There have been uncountable social networks formed but only a few has finally achieved their true goal/s, which emphasizes the complexity of such a matter.

A social network is usually created by a group of individuals, who have a set of common interests and objectives. There are usually a set of network formulators followed by a broadcast to achieve the network membership. This happens both in public and private groups depending upon the confidentiality of the network. After the minimum numbers are met, the network starts its basic operations and goes out to achieve its goal. Success of a social network mainly depends on contribution, interest and motivation of its members along with technology backbone or platform support that makes the life easier to communicate and exchange information to fulfil a particular communication need.

Implementing social networks and sustaining them is one of the biggest challenges and people have formulated many mechanisms in the past to keep alive such networks. This has been largely supported by the advancements in the field of IT. The large scale computerizations and the powerful advent of E-Commerce have aided this also, but overall, the need for a structured support was and is still there. Web 2.0 has been one of the greatest contributors in this area and it has been a great contributor in the era called ‘technology diminishing the humane distance’.

Question 16

What are the various Components of Web 2.0 for Social Networks?

Answer:

In today's environment, computer literacy is at its peak and tools that are aided through the computerization age are most effective in keeping alive a concept as complicated as Social Networks. The beauty of Web 2.0 fitment to Social Networks is that all the components of Web 2.0 are built for the growth and sustenance of Social Networks. Major components that have been considered in Web 2.0 include the following:

- **Communities:** These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are a number of tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.

- **Blogging:** Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.

- **Wikis:** A Wiki is a set of co-related pages on a particular subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.

- **Folksonomy:** Web 2 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.

- **File Sharing/Podcasting:** This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.

- **Mashups:** This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mob service provider and the map facility of the Google maps in order to find the exact information of a cell phone device from the internet, just by entering the cell number.

As we see from the above components of Web 2.0, each of them contribute to help the implementation and continued existence of social Networks on a meaningful basis. While wikis and communities help to create an online space for the networks, blogging, folksonomy and file sharing help to information flow across the virtual world of the social networking community.

Question 17

Explain the various types and Behaviour of Social Networks

Answer

The nature of social networks gives its variety. We have various types of social networks based on needs and goals. Compartmentalizing social networks is quite a challenging activity.

Social network exist in various domains-within and outside organizations, within and outside geographical boundaries, within and outside social boundaries and many other areas. Such huge variations make the reach of social networks grow to all sectors of the society. Keeping these in mind the main categories identified are given below:

- **Social Contact Networks:** These types of networks are formed to keep contact with friends and family. These have become the most popular sites on the network today. They have all components of Web 2.0 like blogging, tagging, wikis, and forums. Examples of these include Facebook and Twitter.

- **Study Circles:** These are social networks dedicated for students, where they can have areas dedicated to student study topics, placement related queries and advanced research opportunity gathering. These have components like blogging and file sharing. Examples of these include, Fledge Wing and College Tonight.

- **Social Networks for Specialist Groups:** These types of social networks are specifically designed for core field workers like doctors, scientists, engineers, members of the corporate industries. A very good example for this type of network is LinkedIn.

- **Networks for Fine Arts:** These types of social networks are dedicated to people linked with music, painting and related arts and have lots of useful networking information for all aspiring people of the same line.

- **Police and Military Networks:** These types of networks, though not on a public domain, operate much like social networks on a private domain due to the confidentiality of information.

- **Sporting Networks:** These types of social networks are dedicated to people of the sporting fraternity and have a gamut of information related to this field. Examples of these include Athlinks.

- **Mixed Networks:** There are a number of social networks that have a subscription of people from all the above groups and is a heterogeneous social network serving multiple types of social collaboration.

- **Social Networks for the 'inventors':** These are the social networks for the people who have invented the concept of social networks, the very developers and architects that have developed the social networks. Examples include Technical Forums and Mashup centres.

- **Shopping and Utility Service Networks:** The present world of huge consumerism has triggered people to invest in social networks, which will try to analyze the social behaviour and send related information for the same to respective marts and stores.

- **Others:** Apart from the networks outlined above, there are multiple other social networks, which serve huge number of the internet population in multiple ways. Some of these networks die out very fast due to lack of constructive sustenance thoughts while others finally migrate to a more specialist network.

Question 18

What are the various benefits and Challenges for Social Networks using Web 2.0?

Answer:

Web 2.0 has provided a number of benefits to social networks.

Benefits:

- It provides a platform where users of the network need not to worry about the **implementation** or underlying technology at a very **affordable cost** and a very easy pickup time. Concepts of Web 2.0 like blogging are some things that people do on a day-to-day basis and no new knowledge skills are required.

- Web 2.0 techniques are very people centric activities and thus, **adaptation is very fast.** People are **coming much closer** to another and all social and geographical boundaries are being reduced at lightning speed, which is one of the biggest sustenance factors for any social network.

- Using Web 2.0 also **increases the social collaboration to a very high degree** and this in turn helps in achieving the goals for a social network.

Challenges:

- There are a number of challenges that are faced within the implementation of social networks using Web 2.0 concepts. One of the major aspects is data **security and privacy** and in such public domains, there is a huge chance of data **leak and confidentiality** loss because there are usually no centrally mandated administrative services to take care of such aspects. Privacy of individual users also arises and can create a huge problem if malicious users somehow manage to perpetuate the social networks. This is more important for public utility networks like doctors and police.

- A majority of the social networks are offline, and for bringing these under the purview of online social networks, a lot of education and advertising needs to be done, which itself becomes **a cost burden**, when the people involved are not computer literate. This becomes **more viable in the areas of the world that are developing and do not have the basic amenities**. The fact is that these areas are the ones that can benefit the most using social networks in an online mode and a huge amount of effort would be needed to help them using the technologies.

Web 2.0 has introduced a number of powerful features that social networks are utilizing. These have provided significant advances, which can be seen by the worldwide acceptance of networking sites with these technologies. In spite of all challenges, the worldwide acceptance of social networks and its implementation using Web 2.0 is here to stay and flourish. It is up to us to participate in this movement and continue to contribute towards the betterment of the technology and concept for more contribution to the society as a whole.