Book No. 1 (containing 36 pages)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

CA Final ..... Examination

Group No. II Paper No. 6

Subject Information Systems Control & Audit

Number of Answer Books used +1

For use by ICAI only

351497

Q. No.	Please put ✓ against the Questions answered	Marks Awarded (to be filled by Examiner) a	b	c	d	e	Total
1	✓	0	3	2	0		5
2	✓	4	1	1			6
3	✓	2	2	1			5
4	✓	2	2	0			4
5	✓	0	1	0			2
6							
7	✓		3	1	3	4	11
8							
9							
10							
Total							33

Use only Blue / Black Ball Point Pen to write and shade the circles.
AVOID RED PEN.
Write the marks in the boxes before shading the respective circles.

Total Marks awarded

033

Total Marks awarded (in words) Thirty Three

Examiner's Signature

Checked
(initial of the Checker with date)

INSTRUCTIONS TO THE CANDIDATE

Answers are not to be written on this page

nber should be written in figures and words in the allotted space at the right hand corner of the sheet.

oll number should be written in the box in numbers and darken the appropriate circles of the OMR portion provided in the right hand corner of the cover page with **Black / Blue** ball point pen.

3. Fill particulars such as name of Examination, Group No., Paper No. and subject at the appropriate space at the left hand upper corner.

4. Remove the perforated Bar Code sticker of the particular paper from the Attendance sheet and affix the same on the box provided in the right hand corner of the cover page.

5. Since a machine will read the Roll no., please check and ensure that Roll number written in numbers, words and circles darkened are correct. In case any candidate fills this information wrongly, Institute will not take any responsibility for rectifying the mistake.

6. The answers should be written neatly and legibly

7. The answer to each question must be commenced on a fresh page and question number prominently written at the top of each answer. Alternatively, the question number should be distinctly written in the margin.

8. The answer to each question in all parts should be fully completed in one page, or in a consecutive set of pages, before the next question is taken up.

9. Writing of Roll number in place/s other than the space provided for the purpose or writing distinguishing mark, symbols like "OM", "Sri", "Jesus", "786", etc., will tantamount to adoption of "unfair means"

Answer No. 7(b)

HIPPA

1) HIPPA is known as Health Insurance Portability and Accountability Act, 1996.

2) At present India has become hub for outsourcing of Health Insurance related services.

3) This emerges the need for having the knowledge of the provisions of this Act.

4) This Act concerns with avoiding unauthorised Access to Health Insurance Records and data.

5) Following are the 2 levels which talks about the health Insurance issue:

A) **Level-I**: Level I specifies the

Coverage of employees and their family's Health Insurance.

B) Level-II : This level deals with Controls to prevent Health Insurance records from unauthorised access. these are as follows:

a) Administrative Level:

This level control is concerned with hiring. Operating staff of Information system who has necessary qualification and Certificate

(3)

b) Technical Level

It is concerned with use of best hardware, software & network system with access Controls.

Answer No. 7(c)

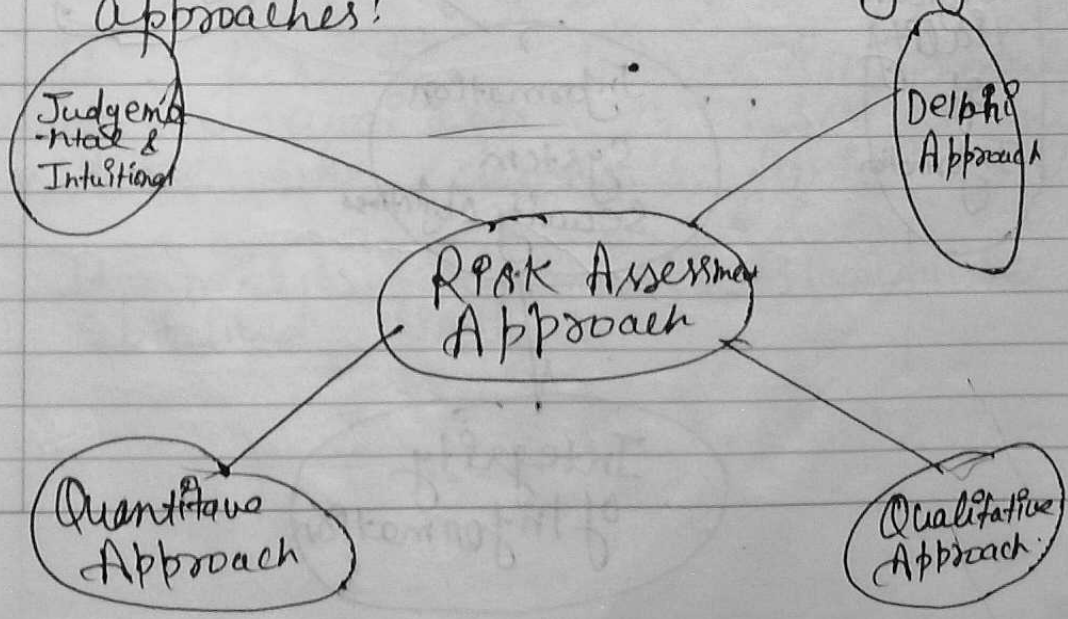
Risk Assessment

1) Risk assessment refers to the extent of risk that an organisation can face if threats exploits the vulnerabilities of the system components.

2) Risk is assessed by 2 factors:

1. Chances of occuring of threats
2. Extent of loss if that threat occurs.

Risk can be assessment by following approaches:

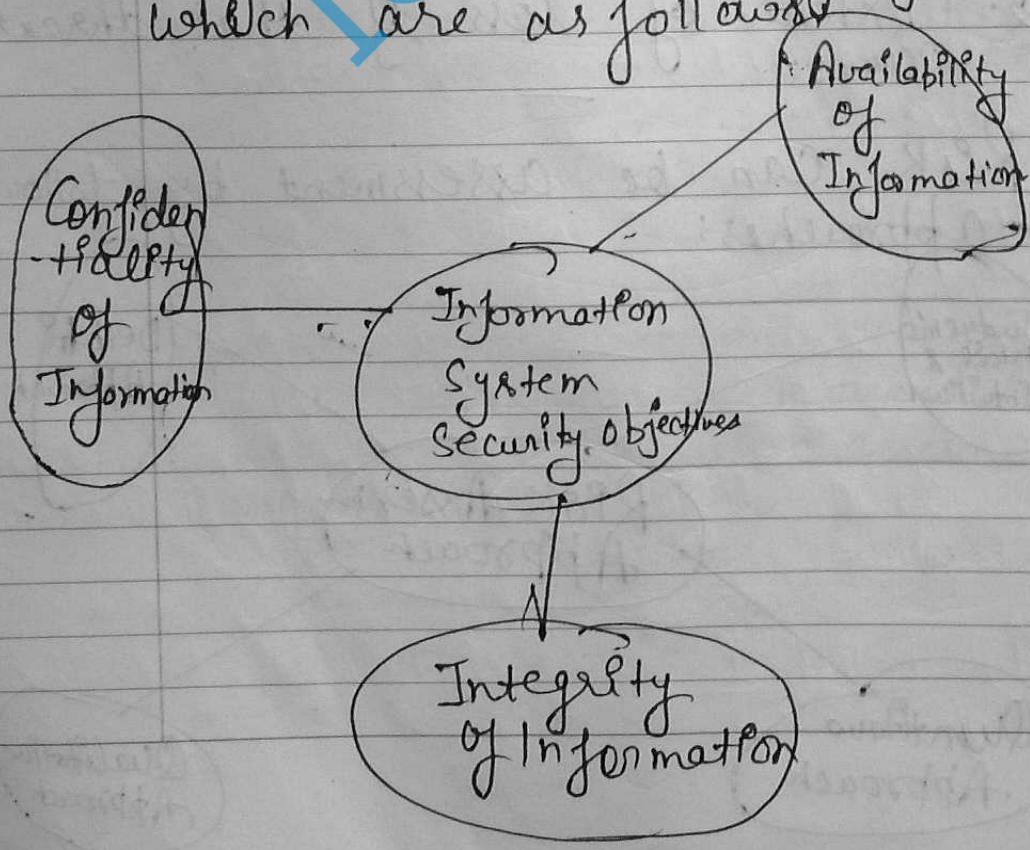


Expected Risk = Probability of Threat (P) × Extent of Loss (E)

Answer No- 7 (d)

Information System Security Objective :

There are 3 objectives of Information Security System which are as follows:



1. Confidentiality of Information

Confidentiality of Information is concerned with Non-Disclosure of User's Information to Unauthorised Persons-Except for legal obligation.

2. Integrity of Information

Integrity of Information refers to "Information should be free from errors and it should have transparency so that it can be trusted and should be free from biasness.

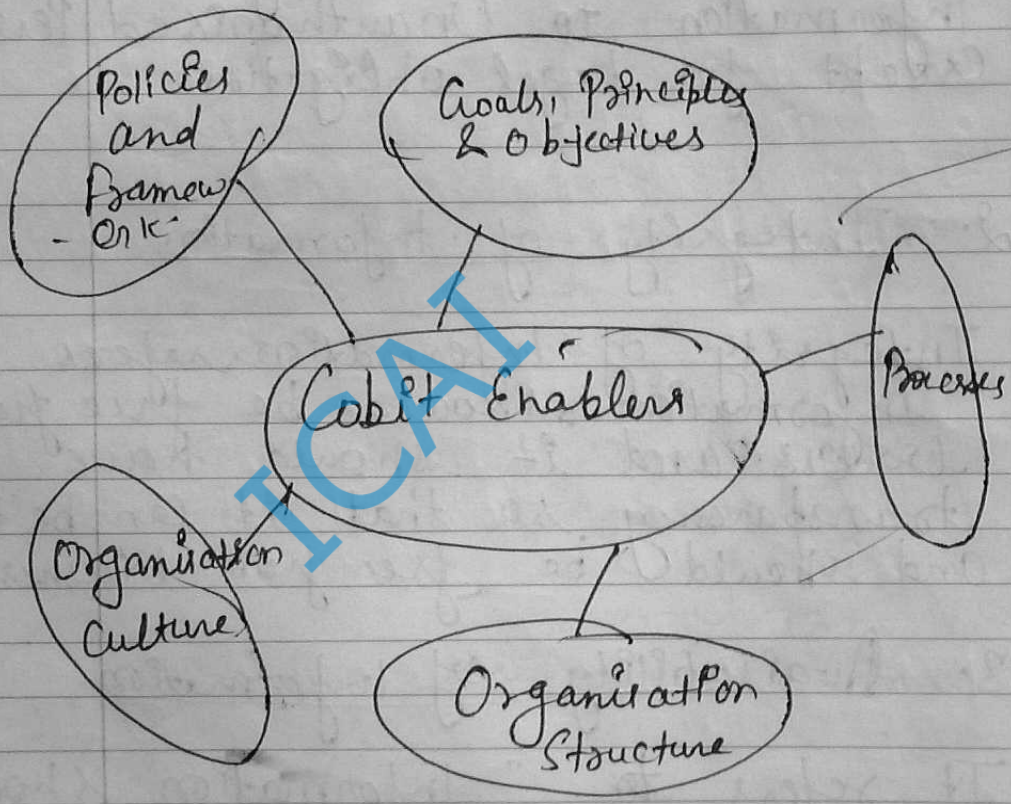
3. Availability of Information

It refers to "Information should be available to user at any time he demands for it.

(3) It means information should be obtained timely.

Answer No. 7(e)

Cobit 5 enablers: Following are Cobit 5 enablers



1. **Principles Goals and Objectives**

Organisation's goals, Objectives and principles enable the management and governance to achieve 5 objectives of COBIT.

2. Processes

Organisation process refers to the sequence in which work is performed. It also enable the management & governance to achieve COBIT objectives.

3. Organisational Structure

It refers to the hierarchy of Organisation and segregation into various departments.

4. Organisational Culture

It refers to the internal work culture of the Organisation in which it works.

5. Employees -

Employees of the organisation also enable to achieve Cobit 5 priciples.

Answer No - 3 (a)

Encryption

1. Encryption refers to coding normal text / data into Cipher Text / data to protect the data from hackers for transferring into Communication Channels.

2. When Hacker hacks the encrypted data, it will not be understood by him and he can not decode it and therefore data will be secure from theft.

3. Encryption is done by set of algorithm called Cryptosystem.

4. Encryption is of 2 types

Encryption | Decryption

Difference between Private & Public Encryption

Private Key Encryption

When Encryption as well decryption is done by a single private key it is known as Private Key Encryption.

Example

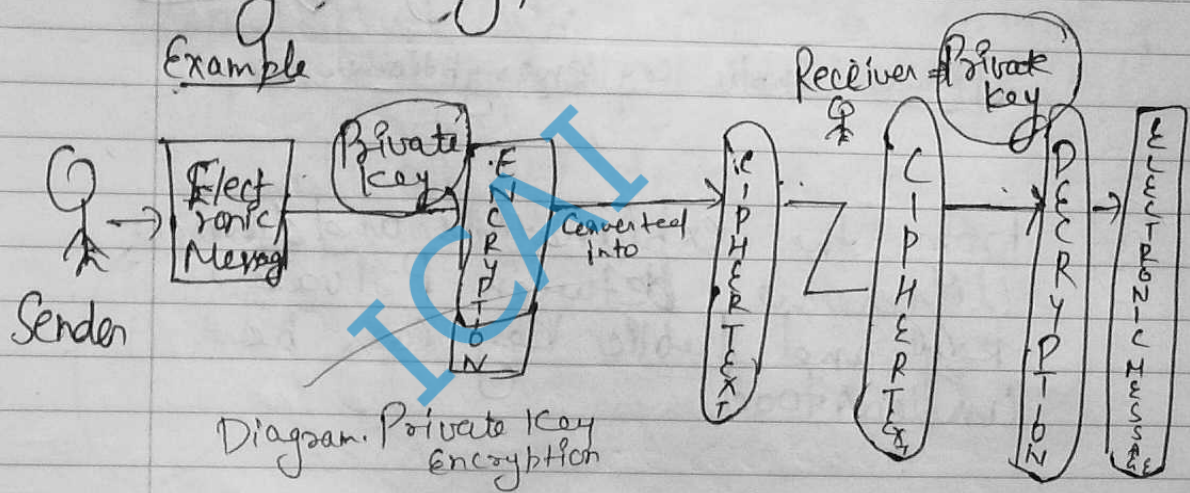


Diagram. Private Key Encryption

Public Key Encryption

1. When Encryption is done by Public key of Receiver and Decryption is done by Private key of Receiver, it is known as Public key Encryption
2. It means Encryption & decryption are done by different keys.

Example ⇒

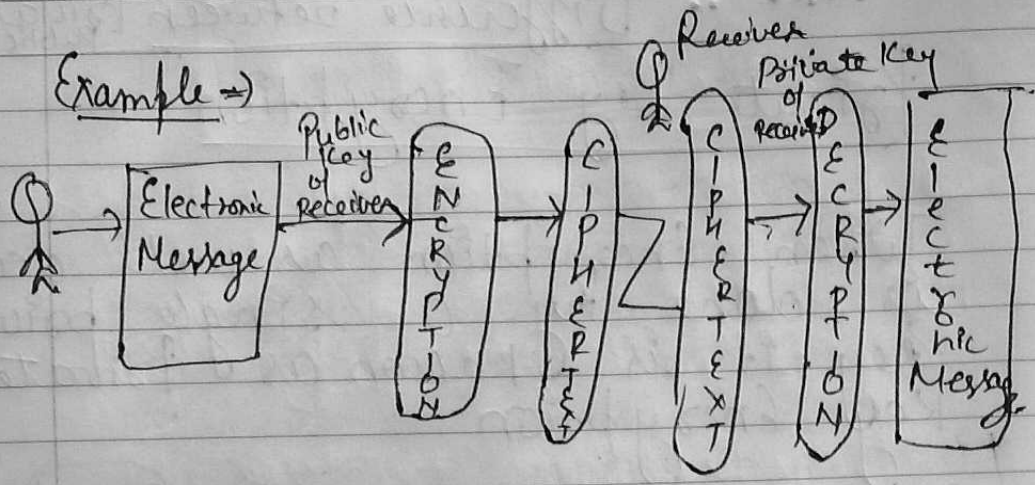


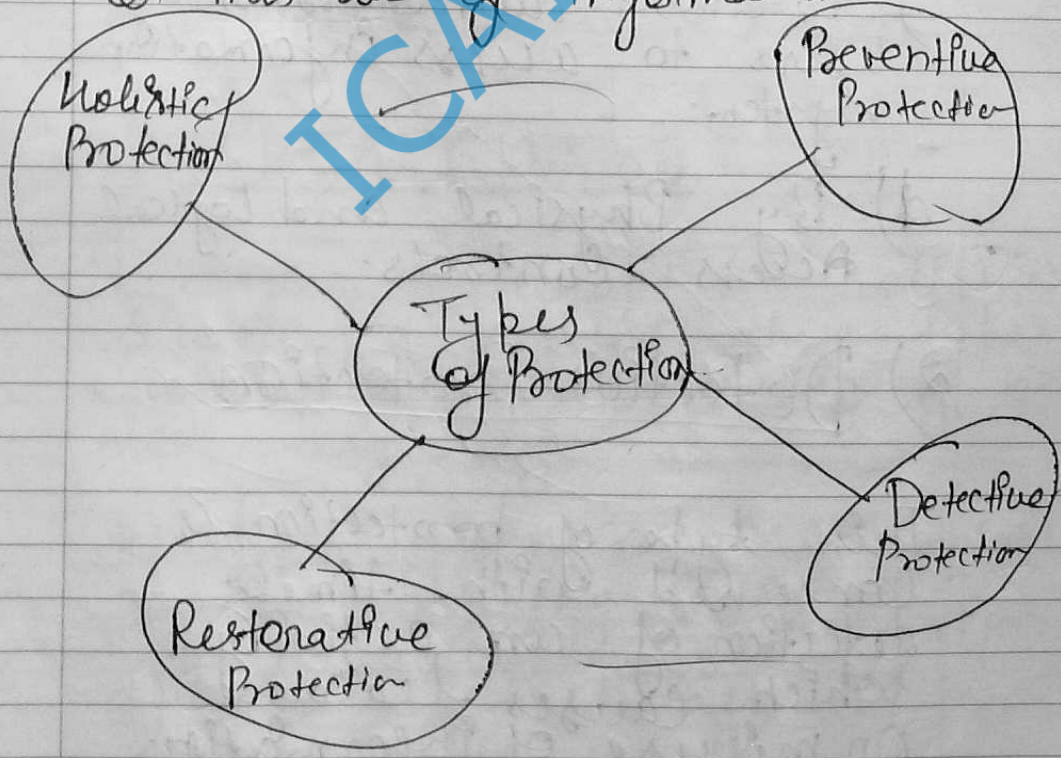
Figure: Public key encryption.

(v) From the explanations and diagrams difference between Private key and Public key can be understood.

Answer No 3(b)

Protection to Prevent leakage or Misuse of Information:

In a computer-held information system, an organisation can use following types of protection to prevent leakage or misuse of information.



1) Preventive Protection

This type of protection refers to the measures for preventing leakage or misuse of information these can be!

a) Use of Antivirus or firewall.
b) Authentication of users by ID, Password etc.
c) Determine authorisation of users to access information system.
d) By Physical and logical Access Controls.

2) Detective Protection

This type of protection is concerned with timely detection of an activity which causes leakage or misuse of information.

example: Detecting

abnormal transfer of Packet from public network to private network with the help of Network Intrusion System.

3) Restorative Prevention

It refers to the process for restoring the data lost or theft.

For example ⇒ Back up plans.

4) Holistic Approach

It refers to adopt an holistic system to prevent these types of events of data leakage, or data theft by.

a) Risk Assessment Methodologies
b) Establishing Controls.
c) Establishing security Policy.
d) Training to staff to prevent from these events.
e) Timely evaluation & Corrective steps to be taken also.

(2)

Answer No. 3(c)

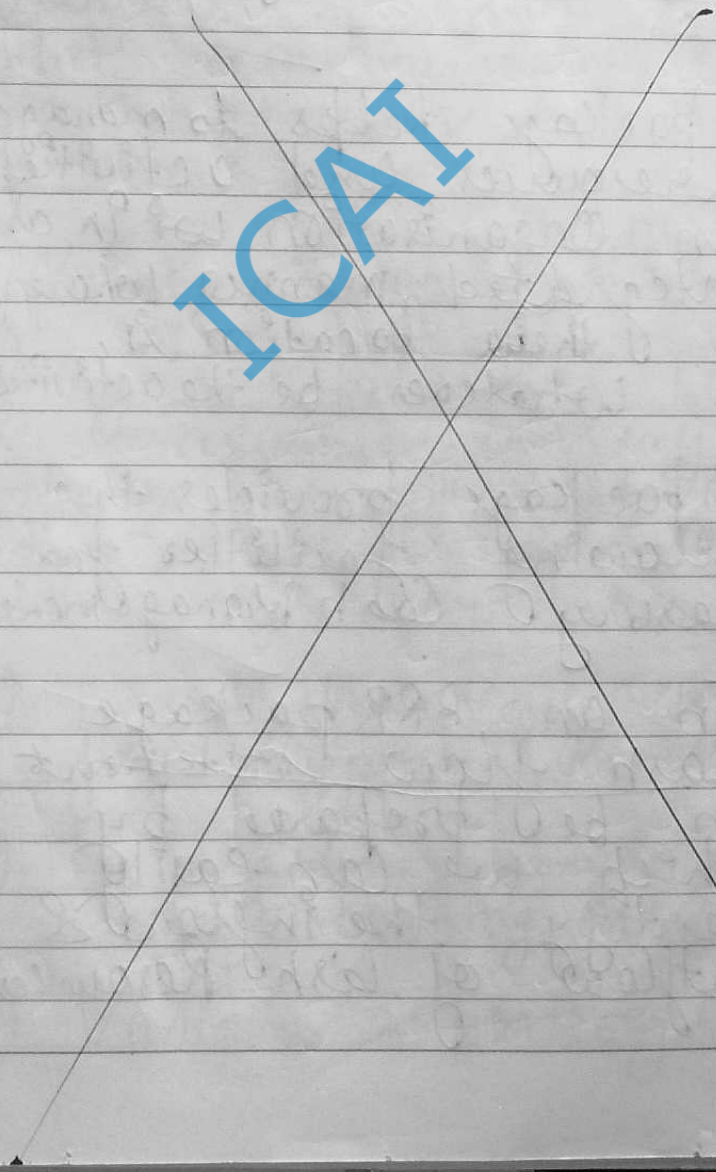
Disaster Recovery Planning for Information Technology Assets:

The following concerns are required to be addressed for Disaster Recovery Planning for Information Technology Assets.

1. First of all Identify the key potential assets of the company.
2. After that assess the threats likely to be occured for those assets.
3. Assess the vulnerabilities of these assets to the particular threats.
4. Identify the extent of loss that can be occured if disaster happens.

5. Identify the controls for security of these assets and also

(1) 6. Plan for immediate recovery of these assets after the disaster.



Answer No. 2(a)

Facilities available in Treasury Cash Management of an ERP Package:

ERP package helps to manage the resources and activities of an Organisation within an integrated manner where ever the location is, and whatever be the activities.

ERP package provides the following facilities for Treasury Cash Management.

1) In an ERP package Cash flow statement can be prepared by which we can easily identify the inflow & outflow of cash Resources.

2) Since ERP is an Integrated system, the Cash transactions, balances of all the branches, locations are available ~~in a~~ string at everywhere (branch/location)

3) Since ERP is also Multicurrency, Multicountry system, it will provide the cash amount in required foreign exchange / domestic currency.

4) It enables to maintain Bank Reconciliation Statement.

5) If Enterprise has 'IOU' system. i.e. advance to staff for any expense; it will help in recovering the amount and will prevent to issue IOU beyond the limit.

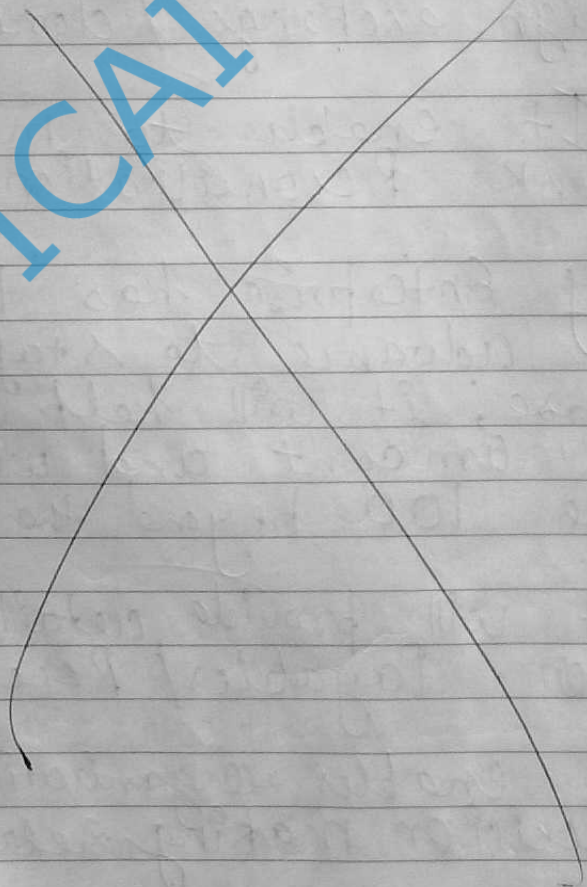
6) It will provide details & reports for Payables / Receivables.

7) It enables organisation in decision making related to Cash

8) Various reports eg. Cash

Gross, Cash Excess, Cash Current Ratio will be made by ERP.

(4) 9) Hence we can say that ERP package is a big facilitator for Treasury Cash Management.



Answer No- 2 (b)

Issues to be addressed in "Access Control" under Information Security Policy :

The following issues are addressed in access control for information security policy.

1. Authentication of users of Information system by using ID/ Password, PIN, User Id etc & Smart Card and by allowing access by thumb impression etc.

2. Authorisation for access to Information system:

User should be authorised for access to information system by using list or Ticket for authorised data.

3. By Installing Antivirus and Firewall, unauthorised access will be prevented.

4. Data Intrusion System
5. By Network Address Translation Network can be saved from.

6. Lock on doors

7. CCTV Camera.
8. Provide policies & guidelines to employes not to involve in unauthorised access / control.

9. Installation of single door Entry.

(1) 10. Deadman Doors

Above are the measures which can be taken for Access Control under Information Security Policy.

Answer No 2 (c)

Waterfall method is the traditional model of System Development life cycle.

Strength of Waterfall Model:

1) It is a simple model and easy to develop.

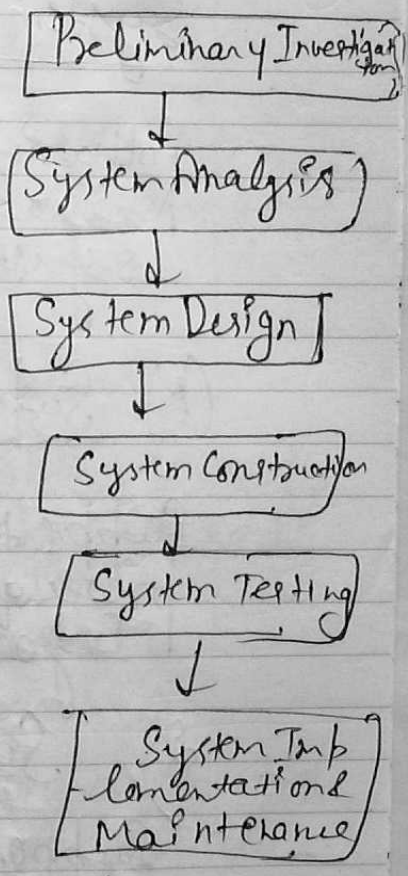
2) Provides sequence of activities which helps developer to work in systematic Manner.

3) Chances of Error are low after implementation.

4) Easy to understand.

5) Low cost model.

6) Speedy Development



Waterfall Model

Answer No-5(a)

Major Prerequisites of a Management Information System:

Following are prerequisites for Management Information system:

(1) Support of Staff

Support from staff is a prerequisite for Management Information System.

2) Support of Management

Support from management should be there for a successful Management system.

3) Management Directed

Management information should be management directed so that it will be implemented.

4) Management oriented

MIS should be developed with specification of management what they want in it.

5) Flexibility

MIS should be flexible so as to adapt the changes to be occured in future.

6) Exception based:

It should be exception based and should have query option.

7. Proper Hardware & Software

Proper Hardware & software should be installed before MIS.

Answer No. 5(b)

Various Categories used in System Development life cycle of Software Maintenance:

⇒ After implementation of system the work of organisation does not come to an end.

⇒ It should now tend to see system maintenance.

⇒ To ensure system maintenance Organisation should do following measures.

1) Periodic evaluation of system performance should be done.
2) If there exist any irregularity system developer to be informed.
3) Corrective measures to be taken for improving the system
4) Staff should be given training to work in system in an efficient manner.

Answer No-5 (c)

As the provisions of Information Technology amendment Act. 2008, the persons liable for sending Obscene to ~~every~~ any person will be liable to be guilty under this Act.

In the given Question, Mr A is regularly sending obscene in electronic form to Ms. B through XYZ network service provider.

As per the provisions ~~for this~~ of the Act, Intermediary will not be held liable if he proves that the offence was committed without his knowledge and he was not party to the Act.

Hence in light of above discussion it can be concluded that

⇒ Mr A will be held liable in this Act.

⇒ XYZ service providers will be held liable if he fails to prove that the offence was committed without his knowledge.

⇒ If XYZ service provider will prove that he was unaware of the offence he will not be held liable in this Act.

(1)

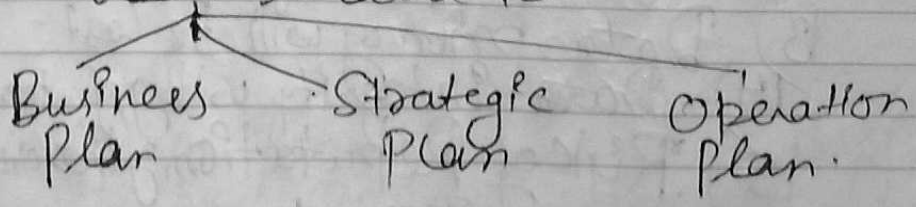
The offender will be liable for fine or punishment of imprisonment or both.

Answer No - 4 (a)

Threats to the Computerised Environment due to cyber crimes

The following are the threats to the Computerised system due to Cyber Crime:

1. Unauthorised Acces to data.
2. Modification, Deletion and alteration in data.
3. Identity Theft.
4. Hacking.
5. Cracking.
6. Risk of Theft of sensitive data related to



7) Cyber Terrorism Risk

Terrorist can use the IP address for their terrorist activities.

8) Competitors can steal innovative strategies, Quotations etc.

9) Productivity of system can go for a toss by virus attacks.

10) Leakage of E-fund transfer password can also be hacked.

11) System will stop working.

12) Alteration in Protected files can be done.

13) Data privacy will be lost.

14) Data Integrity will go for toss.

15) Risk of Reputation, Financial or Legal loss.

Answer No. 4 (b)

Advantage of Continuous Audit Techniques:

Following are the advantages of Continuous audit techniques.

1. Audit will be comprehensive and detailed.
2) Possibilities of errors and frauds will become low.
3) Continuous Audit Techniques will help in directing employees to work error free and in efficient & effective manner.
4) There will be no sampling risk.
5) Auditor became aware of all the procedures & systems of the organisation and hence

will become specialised in that field and can also helps management to advice on certain matters.

Disadvantage of Continuous Audit Techniques

1) Audit assignment will be tedious.

2) Productivity of Auditor will bring down due to boredom.

3) Employees of the Organisation will get demotivated by excessive checking.

4) Continuous audit techniques have disadvantage to the Organisation in a manner that staff who help the auditor in his work will not be able to do his work in organisation and hence loss to organisation

Answer No. 4(c)

Methodology of developing Business Continuity Plan

The following is the methodology for developing business continuity Plan.

1. Preplanning.
2. Vulnerabilities in the systems are identified.
3. The probability for occurence of threats to the system is identified.
4. The expected loss to the system is identified.
5. After Evaluating the risk Controls are set.
6. After that design of Business Continuity Plan is made.

7. After the design is made, then this Business Continuity Plan is tested.

8. After Testing the design of Business Continuity Plan, it is implemented in the system.

9. After Implementing its periodic Inspection is done to maintain it and Corrective actions is taken if there exist any error Or Chance of improvement is there.

Answer No. 1 (a)

System Requirement Specification

System Requirement specification document is made ~~after syst~~ in the step System Analysis of System Development life Cycle.

Contents of SRS for a typical Software development

1. Description of existing system design & its problems.
2. Requirements of users in existing system design. (Need of users)
3. User's Need & specification.
4. Problems in existing system.
5. Design of system avoiding problems with of existing system incorporating user's requirements.

6. The existing system with problem described in a flowchart

7. The Required system with possible user's needs described in a flow Chart

8. And also use of ER Diagram

Answer No. 1 (b)

Provisions for retention of Electronic Records under Section 7 of Information Technology Act, 2008:

Section 7 of Information Technology Act (Amendment) 2008 states the following provision for retention of electronic records.

1. Records should be maintained in their original form.

2. Records should be accessible to users whenever he requires.

3. Additionally, there are also following requirements which requires to retain

a) Date of Receipt of Electronic Record.

b) Time of receipt of Electronic Record

c) Originator Name (Address I.P.)

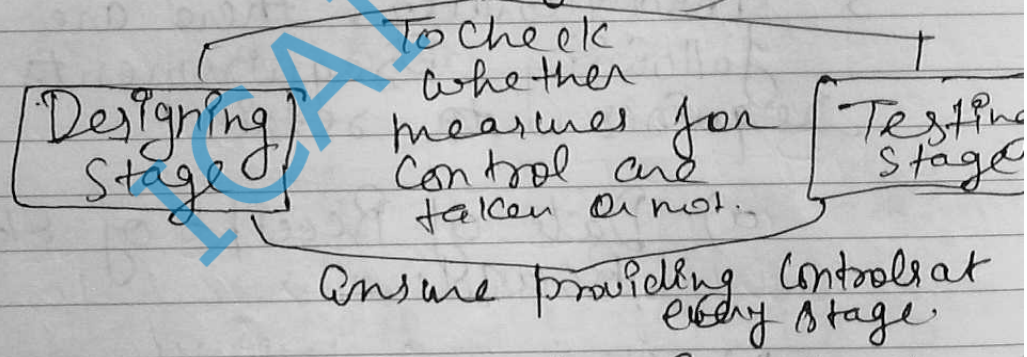
(3)

Documents should be accessible to authorised users only.

Answer No- 1(c)

Role of Auditor in information processing system design throug SDLC :

The Role of auditor in Informat processing system design throug SDLC is as follows :-



1. The auditor's role in system development life cycle star from designing and to Testin stage.

2. Auditor's role is to check whether measures for contr ie control procedures for threaths has been taken into consideration or not.

3. Auditor has to report if no control measures taken for designing & Testing stage in System Development life cycle. (2)

Answer No. 1(d)

Controls and objectives of System development

1) Security requirements should be identified and provides controls at every agreed prior to the development of Information System.

2) In System Analysis, system developers assess the risk involved and threats to be occurred while developing the system.

3) Hence system developer specify and provide controls at every stage of system development life cycle.

4) Since if ignorance in providing controls occurs from beginning of system development, system will be more vulnerable to threats

5) And hence sensitive to threats

6) Hence for security of system controls should be established from beginning of System Development life cycle.

7) Hence Controls should be established throughout the entire life cycle of System Development.