INFORMATION SYSTEMS CONTROL AND AUDIT

SHORT NOTES

HAND WRITTEN

Sumit Rathi (CA, Bcom.)

THINGS TO BE KEPT IN MIND EVERY TIME YOU TAKE ISCA BOOK:

1. ISCA is not a technical/computer subject INFORMATION SYSTEMS CONTROL AND AUDIT by its name itself, it is an AUDIT subject and the word COMPUTER is hardly even used in the ICAI material.
2. This subject is to educate an auditor to audit various information system plans in place in an organization, and related controls (to audit information system one should know it).
3. It is subject where maximum marks can be scored –
    1. only 8 chapters
    2. relatively less to study
    3. Normally about 80% of marks are covered from 4-5 chapters.
4. They test knowledge but memory – take best use of your grammar knowledge, draft smart sentences to answer a question.
5. Answer need not be 100% same as ICAI suggested answers, but if smart sentence and key words are used, marks will be allotted.
6. Read the question properly, don't get confused by synonyms used in the question– make note of key words that helps to know the correct answer for a question.
7. Refer previous 8 to 10 attempts question paper, most of the times questions asked in exams prior to 2-3 attempts may be lifted as it is for about 10-15 marks.
8. You may do a rough study of the questions asked in immediate last attempt, normally there will not be repetition of those questions the exam – you will save your time and can focus on other topics. (*disclaimer – exceptional cases questions are lifted directly form immediate preceding attempt's question paper for about 5-10 marks)*
9. Use dictionary to understand the meaning of unknown/new words, don't mug up.
10. Read, write, revise and write.
11. Prepare for 100 marks, attempt for 100 marks.
12. Don't generalize the answer, keep it specific and to the point – quality & quantity both are important.
13. Read case studies from the practice manual and RTPs – same case study may not be asked in exam, but can expect similar questions.

Chapter wise important topics:

Chapter : 1 (Around 5-10 marks)

1. COBIT 5 –Benefits and Component (V imp..)
2. Key Governance practice of GEIT.
3. Internal control component of COSO.

Chapter : 2 (Around 15 marks)

1. Classification of system.
2. Attribute of information.
3. Characteristics of MIS, prerequisites of MIS (5 pillars),limitation and constrains of MIS.
4. EIS definition, Characteristics of EIS, measures and indicators to be included in EIS. (V imp..)
5. Expert system, benefits, characteristics and usage.
6. DSS, characteristics and applicability. (V imp..)

Chapter : 3 (Around 20 Marks)

1. Types of Information system. (imp..)
2. Component of security policy.
3. Impact of technology on internal control.
4. Component of internal control. (V imp..)
5. Components of Controls, Data Integrity Policies, Cyber Frauds-Types of cyber attacks & techniques.
6. Internet & Intranet Controls, Firewall, Cryptography, Access Control Mechanism, System Development Controls & Computer Centre Security Controls as a part of General Controls.

Chapter : 4 (Around 12 marks)

1. BCP deviation, methodology of BCP. (V imp..)
2. Business impact analysis.
3. Types of backup.
4. Objectives of BCP. (imp..)

Chapter : 5 (Around 20 marks)

1. Fact finding techniques.
2. System implementation conversation strategies.
3. Post implementation review. (V imp..)
4. System development methodology.
5. Methods of system development. (V V imp.. especially waterfall, incremental and spiral).
6. Methods and grounds of vendor evaluation, Roles involved in SDLC
7. System testing.

Chapter : 6 (Around 15 Marks)

1. Functions of Auditor.
2. Categories of IS Audits (V imp..)
3. Concurrent Audit Tools(especially SCARF, Audit Hooks). (V imp..)
4. Critical Factors to be considered by IS Auditor in Preliminary Review of IS Audit, Approaches to Application Security Controls Audit. (V imp..)

Chapter : 7 (Around 8-10 marks)

1. System Audit & Controls of IRDA & RBI, Cyber Security Policy 2013, Objectives (V V imp..)
2. ITIL
3. Penalty sections etc..

Chapter : 8 (Around 10-12 marks)

1. Cloud computing, objectives, characteristics of cloud computing, advantages of cloud computing (V V imp..).
2. Benefits of Mobile Computing, BYOD,Types of Social Networks, Components of Web 2.0 (V imp..)
3. Disadvantage of cloud.
4. Pertailmaint issues in cloud computing. (V imp..)
5. Cloud v/s Grid computing.

ISCA

CH-2

(1) System -> orderly arrengment - interrelated & independent - Element.
* operates collectivelly - for some common goal.

Types :-

According to Element

(1) Abstract System / Consaptual System.
↓
Arrengment of Independent Idean.

(2) Physical System :-
Tangible elements for common goal.

Ex :- Circulatory System - HART - VESSELS - .
School System . - BUILDINGS - TEACHERS - Administration - Books - etc.

Intraction Based

(1) open System :- intracts freely & Changes with Environment
(2) Closed System :- non-intractive & non-changing.
↓
Not available as such - But often available in Physical System.

Human Intraction

(1) manual System :- (1) DATA COLLECTION.
(2) Manipulation
(3) maintenance - &
(4) Final reporting
} Carriedout by Human efforts.

(2) Automated System :- All the (4) above are carried out by Computer.
But to Some Extent human efforts are required.

~~① System~~

working & output

① Deterministic System. → operates on predictable manner, wherein interaction amongst the parts is known with CERTAINITY.

② Probabilistic System → operates on probable behaviour & certain degree of error is always attached.

⇒ Attributes / characteristics / qualities of Information :-

imp

① Should be available (Availability) on the time when needed.

② Basic Purpose (purpose) is to inform, Evaluate, persuades & cognize.

③ Mode (mode & format) :- Should be visual / verbal / written form

↓

So as to assist in decision making, Solving probs, initial planning, Controlling & Searching.

④ Information should always Latest (Decay) with the time. (decay)

⑤ Should be Complete as much as possible (completeness)

⑥ Correctness & Realistic. (correctness, frequency)

② MIS (Management Information System) :-

it is → Integrated user machine system.

Disigned to → Providing information.

to → Support operational ~~control~~ Control, Mgt. Control, & Management function.

Characteristics of MIS

(1) Integrated → i.e Subsystems from operational level to functional level are linked to provide info.

(2) management oriented.

(3) Management Directed :- as mgt oriented, mgt should review at all stage & also ensure the implementation of System.

(4) Sub systems → i.e many subsystems providing ground level info. for batter performance,

(5) Heavy planning Element :- To avoid System obsolensce

(6) Could be non-Computerized, but Computerized give more efficiency & Effectivness.

(7) Common database & Common dataflow.

⇒ Pre-requisites of MIS :- 5 Pillars

(1) Data base :- i.e a Super file which Consolidate the data, which are formally stored in many file.

↓

- Such database Should be User-oriented
- Should act as Common data Source for various applicents.
- accessable to authorized person only.

(2) Qualified System & management Staff :-

- Involve experts from relevent areas.
- maintain good Co-ordination b/w System & mgt. Experts.
- mgt. Should guide the Expert to develop the system according to its mgt's requirment.

③ Support from Top mgt:

④ Control & maintenance:- MIS should be operated into, in ~~the~~ accordance with the written down procedures, rules & methods. mgt. should check the system at every stage & have a close watch on it to avoid the methods of short cut used by users some times, which will reduce the effectiveness.

⑤ Evaluation:- MIS to be effective, should be capable of meeting the information requirment in future as well. So mgt should evaluate & examin:-

① whether enough flexibility exist in the system, to copup (copeup) with any expacted/unexpacted info. requirment in future.

⇒ limitation of MIS → means → the max. MIS can be used
i.e How much best MIS can produce.

⇒ Constran in operating MIS → means → problems faced or to be face
@ may be faced while using MIS.

③ Executive information system:

- its a tool, that provides
- Direct online access, to the relevent info.
- in a useful & navigated formate
- about aspects of busines.
- to the senior manager.

- Characteristics of Executive info. System

① Computerised, → providing → needs to top mgt.
② Capable a accessing internal & External data.
③ Provide (Rapid Acces) to the timely info.
Provides Direct Acces to mgt. Report.
④ Tool for decision making.
⑤ Provide online analysis tool like trend analysis etc.

⇒ Principles → to guide → the design of measures & indicators → to be included in an EIS

↓

① EIS measures should be able to meet the changing Environment & need of organization.
② EIS measures must be easy to understand.
③ it should Collect data from where-ever ponible. & Should not add Substantially on the workload of Staff & mngr.
④ EIS measurs must be based on balanced view of org's objectives
⑤ Data System Should reflect the objectives of the org.
⑥ EIS info. must be available to every one, other than Confidential matters.
⑦ EIS measurs must encourage mgt. & Staff. to share the ownership & responsibility of org. objectives.

(4) 100% question

Expert System :-

They are designed to replace the need of a human expert, they are particularly important where human expert is scare, & therefore expensive.

They imitate the process of human experts & provide the decision with reason, with the type of advice, that normally is provided by human experts.

It Express the knowledge on the facts & rules.

⇒ Business Application (not benefits) of Expert System :-

Area	Application
(1) A/cing & finance -	i) provide tax advice. ii) helping with Credit authorization. iii) Provide investment forecasting models. iv) Investment related advice.
(2) Marketing -	i) Provides automate enquiry of Customers. ii) Telemarketing. iii) Price quotations etc. iv) Latest product info.
(3) manufacturing -	i) Computer assisted Processing (CAP) & production. ii) Quantity analysis. iii) Job work scheduling etc.
(4) Personnal -	i) helps into evaluating Employee's performance.
(5) General busines -	i) acquisition Strategy formation. ii) training etc. iii) Evaluation etc.

→ Benefits of Expert System

(1) Knowledge of Expert can be preserved, even if they leave org.

(2) It helps new people (novices) to accumulate knowledge & help in making expert decision.

(3) Can be effectively used in reducing cost, marketing strategies, manpower planning etc.

(4) Real-life support can be obtained from Expert System.

⇒ Properties that a potential application should possess to qualify for expert system Development ↓ (or) Characteristics of ES:

(1) Availability: Expert System can provide, through reasoning, how to solve a problem, with an example for better understanding.

(2) Complexity: It helps to solve complex problem, with logical inference.

(3) Domain: The subject area of Expert System is well defined.

(4) Expertise: The knowledge of Experts is modeled & kept.

(5) Structure: The solution process must be able to Copeup with ill-structured, uncertainity, etc.

(5) Office Automation System :-

OAS is rapidly expending newest Computer based information System, that helps in saving Costs & times etc. otherwise wasted on by human for doing the same job.

→ Benefits of OAS :-

(1) Improves Communication, within & with other orgnizations
(2) Reduce the time taken for process.
(3) Reduce Costs of Communication, etc.
(4) Provide high degree of acuracy & Reliance.

(6) Computer Based Information System :-

CBIS is an information System in which Computer plays a major role. Such System Consists of following Components

(1) Hardware,
(2) Software.
(3) Data - Raw facts & figures, which are stored in secondary device.
(4) Procedure - Step by Step manner to achive output
(5) People - user, analyst, administrator etc.

→ Characteristics of CBIS

(1) Predetermined objectives
(2) integrated - All Subsystems are Interconnected
(3) has numbers of Subsystem
(4) any one Subsystem fails - normally System as a whole fails.
(5) Subsystem's goal are lower than Entire System's objectives.

(7) Transaction Processing System: (TPS):

TPS is a System that Collects data from business transaction (i.e sales, purchase etc) & these data are organised & manipulated to generate various information for the product for external use.

→ Activities involved in TPS:

Capturing data & organizing in files/database

↓

Processing the file/database using application software.

↓

Generating information in form of report, &

↓

Processing queries from various quarters of org.

→ Components of TPS

(1) Input, (2) Processing, (3) Storage (4) Output.

→ features:-

(1) Large volume. (2) Automation of Basic operations
(3) Source of input for other process/system.
(4) Easily measurable

(8) Management Support System (MSS):-

it is an information system which Support managers in effective decision making by providing relevent & required information at the right time & to the right people.

→ Types: (1) Management information system.
(2) Decision Support System.
(3) Expert System

⇒ Basic Components of message Communication

① Electronic mail . ② Facsimile (Fax) ③ Voice mail

imp ⇒ features

① Portability - i.e accessable from any Computer.
② Online development & editing possible.
③ Electronic Transmission, & quick transmission.
④ Economical.
⑤ Integral with other information System. Such integration helps in ensuring that the msgs are accurate & the information required for the msg is accessed quickly.

⑨ Decision Support System : (DSS)

It is a System that provides tools to management / manager to assist them in Solving Semi-finished & unstructured problems in their own somewhat personalized way.

DSS is not inteded to make decision for managers, but rather to provide managers with a set of Capabilities that enable them to generate the info required by them in making decision

⇒ Areas for Applying DSS :

① Cost Alcig System.
② Capital Budgeting
③ Budget variance Analysis System
④ Generate decision Support System.

⇒ Characteristics of DSS :

1. It Supports decision making & occurs at all level of mgt.
2. It should be flexible & adeptable.
3. It focuses on decision rather than data info.
4. It should be easy to use.
5. It can be used for structured prob.
6. It should be user frandly.
7. It is used mainly for decision making.
8. Dss's impact on Decision where manager's judgment is essential.

CH-3 ISCA

⇒ Security objectives: The Security objective is to protect the interest of those relying information: ~~info. System & Communication which delivers the info.~~ & protecting such info. from harm resulting from failure of ① Integrity ② Confidentiality & ③ Availability.

① Integrity → unauthorized modification
② Confidentiality → unauthorized Disclosure
③ Availability → unauthorized withholding.

⇒ Types of Info. Security policies & their hierarchicals (ICAI United Nation.)

① Information ~~System~~ Security policy :- This policy provides a definition of info Security its overall objective & importance applies to all users.

② Condition of Connection :- this setout a group policy for Connecting to their network. it applies to all orgs. Connecting to the group.

③ Acceptable usage policy :- This sets out the policy for acceptable use of email & Internent Service

④ Information classification policy :- this policy sets out the policy for the classification of information.

⑤ User Security policy :- This policy sets out Responsibilities & Requirments for all IT system users.. it provides Security terms of reference for users, line managers, & System owners.

⑥ Network & system Security policy :- This policy sets out detailed policy for System & Network Security & applies to IT Department users.

⇒ ~~Import~~ Components of Security policy :-

A security policy must clearly state the following :-

① Purpose & Scope of document & intended audiance.
② The Security infrastructure.

(3) Security org. Structure.
(4) Inventory & classification of Assets.
(5) Physical & Environmental Security.
(6) Identify management & access Control.
(7) IT operation mgt.
(8) IT Communications.
(9) System development & maintenance Control
(10) Business Continuity planning.
(11) Legal Compliances.
(12) monitoring & auditing requirment.
(13) underlying technical policy etc.

⇒ IS Control :-

Control is defined as policies, practices & enterprise structures → that are designed → to provide → reasonable assurance, that the busines objectives will be achived → & undesired events are → prevented, detected & Corrected.

An IS audit includes reviewing the implemented System (or) providing Counsultion & evaluating the reliability of professional effectiveness of Controls.

⇒ Impact of IT Technology on Internal Control :-

The internal Control of an org. with regard to Computerized enveronment is to safegaurd assets, data integrity, System efficiency, effectiveness :- & that can be achived by.

(1) Personnel - Should have proper Skill & knowledge.
(2) Segragation of duty :- even of IT Department people.
(3) Authorigation procedure.
(4) Record keeping.
(5) manggement Supervision & review.
(6) Acces to records / files :- Should be password protected etc.
(7) Control on Storage of data & programs.

⇒ Components of internal Control:

Internal Control comprise of following 5 interrelated Component

① Control Environment: Element which establishes the Control context in which Specific accounting System & Control procedure should operate. It looks @ Controlls the ways in which authority & responsibility are assigned, the functional method of audit Committee, methods of planning etc.

② Risk Assessment:- Elements that identify & analyze the risks faced by an org. & the way the risk can be managed.

③ Control Activities:- Element that operate to ensure transactions are authorized, duties are segregated, adequate documents, records etc. these are called accounting Controls.

④ Information & Communication:- Element in which info. is identified, captured & exchanged in a timely & appropriate form to allow personnel to discharge their duties.

⑤ monitoring:- Element that ensure internal Controls operate reliably over time.

⇒ objective of Controls: The objective is to provide reasonable assurance to achive the objective of busines of org. it aims to minimize or to eliminate the potential loss towards achivement of org objective.

① To reduce the Exposer of ommission of data, etc.
② To reduce the mgt. Lacking in understanding is risks etc.
③ To Control the efficiency in procedure & Comparision etc.

⇒ Catagories of Control:- based on objectives:

① Prevention Control → designed to prevent the errors.
② Detection Control → designed to detect the errors
③ Corrective Control → designed to reduce the impact & take corrective to error detected.
④ Compensatory Control:- Cost of Lock shall not be more than Assets under protection hence use compensatory measures to reduce the cost though they will not be so effective as appropriate control but ok.

⇒ Controls based on IS Resources :

(1) Environment Controls :- they are related to IT environment, such as power, ac, CPU etc.

(2) Physical access Control :- these are related to security of physical IS Resource of intangible resource stored on tangible device. Ex: putting CCTV, Electric door etc,

(3) Logical Access Control :- these are relating to logical access to info. resources, Ex :- Operating System Control, app. Software boundary Controls etc.

(4) IS operational Control :- these are related to control of operation & administration & mgt. of Is operation. Ex : Helpdesks, day end day begin Controls etc.

(5) IS mgt. Control :- Relating to mgt. administration & policies, procedure etc.

(6) SDLC Controls :- Controls relating to planning, designing, testing etc.

⇒ Financial Controls techniqua :

(1) Authorization :
(2) Budget —
(3) Documentation —
(4) Cancellation of documentation —
(5) Input/output verification. —
(6) Safekeeping. —
(7) Subsequent numbered documents. —

⇒ Information classification :- its a Conscious decision to assign a level of Sensitivity to information as it is being created, classification :

(1) Top Secret, (2) Heighly Confidential, (3) Priority.
(4) Internal use only (5) Public document.

① Top Secret: Highly Sensitive internal info. which is classified as top secret & has a very restricted distribution & must be protected all times. (highest Security) Ex: Dgn of mngr, acquisition. etc.

② Highly Confidential:- Info. which is made public or even shared around the org., then Could Seriously impact the org.'s operation & Considered Critical to ongoing operations of org.
Security to these info. is very high, the info. should not be removed without specific authority.

③ Priority: Information of priority nature, procedure, operation work Priorities Project plans etc. security is high.

④ Internal use only: Info. not approved for general circulation outside the org. if such info. is loosed, will Create an inconvenience to org./mgt. but will not lead to financial loss.
Security is normal for this.

⑤ Public document: Information is for public domine. Security is minimal

⇒ Integrity Control:-

To protect the data from accidental or intentional distruction or deletion & provide assurance to user that the expation about the quality & integrity is maintained for info.

↓

Data integrity policies

① Disaster recovery:- A Comprehencive disaster recovery plan must be used to ensure continuity of Corporate bushes in event of outage.

② off site backup storge. must be done.

③ Software testing must be done by installing. (quality test)

④ virus signature Updating:- i.e (entivirus) should be updated immediately when they are made availeble by vendor.

⑤ version 0(zero) Software must be avoided to max possible as they will normally have many bugs.

⇒ Logical Access Control :-

This is a [System based mechanism], used to designate, who can access & what can he access in a System resource, & what type of transactions & functions that are permitted to him

↓

Logical based Control involves evaluating the followings :-

① They restricts the users to use only authorized transaction & functions.

② They are Controls implemented to protect the integrity of the application & the Confidence of the public when public access the System.

⇒ Physical Access Control :- Restricting from entring into an area by unauthorized people :-

① vido cemera, ② Guards, ③ Computer terminal locks ④ Alarm system etc

⇒ Cyber frauds :- major reasons behind Cyber frauds are :-

① failure of internal Control

② failure of mgt. to update themself with new risks.

③ Smart Fraudesto :- who target the weakness of System.

⇒ Type of Cyber frauds :-

① Pure Cyber fraud :- fraud which exists only is cyber world. They are borne out of technology. ex :- website hacking.

② Cyber Enabled frauds :- which can be Committed in physical world but with the use of technology, the size, scale & location of frauds changes :- Ex :- withdrawal of money from Bank a/c by stealing the PIN.

Cyber Attacks :-

① Phishing :- it is the act to attempt to acquire info. such as username passwords, credit card details by representing itself to be a trustworthy entity in electronic communication, or representing it to be a populer web auction site, online payment processor etc. to an unsuspecting public.

② Virus/malicious code :- ITAA 2008 (sec 43) :- Computer virus means, any computer instruction, information, data or program that distroys, damages, degrades or adversly affects the performance of the 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 resources.

③ Network Scanning :- it is a proces to identify the active hosts of a system, for purpose of getting info. about IP address etc.

④ Spam :- E-mailing the same message to everyone on one or more mailing lists is termed as spam.

⑤ Website Compromise / malware propagation :- ie. hosing malware on website in an unauthorized manner.

⑥ Others :- ① Cracking, ② Email forgery, ③ Email threats, etc.

⇒ major techniques to commit Cyber frauds :-

① Hacking :- unauthorizingly accessing the Computer of someone, by mean of technology.

② Cacking :- uneathical is called hacking, & if done for eathical means then called Cracking.

③ Denial of Service (DOS) attack:- It refers to an action or series of action, that prevents access to a Software System by its intended / authorized user.

④ Internet terrorism:- it refers to using internet to disturb electronic Commerce & to destroy Co. & individual Communities

⑤ Logic Bomb & time bomb:-

Logic bomb lies idle until some specified circumstances or Command is not triggered triggered.

Time bomb lies idle until some pre specified time.

- once time or Command occures - it distroys the System & data.

⑥ Data diddling:- Changing the data before, after or during it enters into System.

⑦ Round down:- Round the amount to lower fraction & diff. amount Credit to prepertoor A/c.

⑧ Leakage:- unauthorized copying the data.

⑨ Password Cracking

⑩ **Super Zapping:- it refers to unauthorized use of Special System program to bypass regular system Controls & perform illegal acts

⇒ Boundry Controls:-

The major Control of Boundry System is Access Control mechanism.

Access Control mechanism links the authentic user to the authorized resource which they are permitted to access.

This access Control mechanism has 3 steps:- identification, authentication & authorization.

CH-4

① Business Continuity planning :- (BCP)

it is the Creation & validation → of a particular ~~logical~~ Logical Plan for, how an org. will recover & restor Partially (or) Completely interrupted → Critical function with in a Predetermined time. after a ~~data~~ disaster (or) Extended disruption happend

⇒ Such logical plan is called BCP.

Methodology of BCP :- It Emphasizes on the followings.

① To provide management with a Comprehensive understanding of the total efforts required to develop & maintain an effective recovery plan

② To obtain Commitment from appropriate mgt. to support & participate in the efforts.

③ Defining ~~Developing~~ recovery requirment from the perspective of busines function.

④ Documenting the impact of an extended loss to operation & key busines function.

⑤ Focusing appropriatly on → Disaster prevention.
impact minimization &
orderly recovery.

⑥ Selecting busines Continuity team - that ensures the proper balance required for plan development.

⑦ Finally → Developing a BCP that should be easily understandable & easy to use & maintain.

(8) Defining how, Business Continuity Considerations must be integrated into ongoing Business planning & System development process, in order that the plan remain viable over time.

↓

Eight phases of developing BCP

(1) Pre- planning activity
(2) Assessment of probable ~~dis~~ threats & General Definition of Requirments.
(3) Business impact Analysis.
(4) Detaild defination of Requirment → at this stage develope the profile of BCP.
(5) Plan development → plan all these available option to make the best plan for above all points. & document the same
(6) Testing program.
(7) maintainence program &
(8) Initial plan testing & implementation.

in this phase, probable threat are analysed, the scope of project planning is defined, plan framework is developed & other such aspect.

(1) Pre- planning activity : this phase is used to understand the existing & projected, ~~continu~~ Computing environment in the org.
this enables the ~~the~~ team to,
(1) Refine the scope of project & associated work.
(2) Schedule the project development, &
(3) to identify & address any issues that could have an impact on the delivery & the succes of the project.

→ Steering Committee should be established during this stage, which will provide guidance & direction to project team.

(2) Business impact Assessment - (BIA)

an essential means of systematically assessing the potential impacts resulting from various event or incidents,
this enables the team to :-

(1) identify the Critical System, Critical process & Critical function
(2) to assess the economic impact of incidents & disaster that result in a denial to access the System.
(3) to assess the tolerable downtime @ pain threshold
i.e max time that busines unit can survive without System.

⇒ Different types of Backups :-

(1) Full Backup - taking all files on disk. with every backup generation Contains every file in the backup. [time Consuming & Space Consuming]

(2) Differential Backup :- Here, Backingup those files which are changed since [last full backup]

(3) incremental Backup :- Here, Backingup those files which are chagged since last full / differential / incremental Backup.

(4) mirror Backup :- mirror backup is same as full backup but here [files are not Compressed] in zip file & they [cannot] be protected with password. mirror backup is normally used to Create extract & Copy of backup data.

⇒ alternative procedure for processing BCP:-

for minimizing the impact of disaster, a security mgr should consider the following options.

(1) Cold Site:- if an org is able to / can tolerate some downtime, this is best option. A Cold site will have all facility required to install a mainframe system → i.e Raise floor, A/c etc.

(2) Hot Site:- if fast recovery is critical / important, then use Hot site. All hardware & operation facility will be available at hot site, in some cases software data can/might be stored.

(3) Warm Site:- it provide intermedial level of backup. it has all Cold site facility (+) Even some hardware will also be available.
Ex:- it may have selected hardware (+) a small mainframe that has sufficient power to handle critical situations.

(4) Reciprocal agreement:- two or more org. may agree to provide backup facility to each other. this is cheaper & good.

⇒ Contents of (Disaster Recovery & planning) document:-

(1) The Conditions in which the plan should be activated, & Should discribe the steps / powers to be followed before each plan is activated.

(2) Emergency procedure, which discribes the action to be taken on heapening of an incidate, which should be taken at the time of Effect on busines operation &/or humath life.

(3) Fallback procedures, which describes the actions to be taken to move essential busines activity etc. to alternative temprory location. & action to be taken to bring back busines process back into operation in required time-scale.

(4) Reclumption procedure, to get back into normal line.

(5) A maintenance schedule, which specifies the process of maintaing the disaster plan.

(6) Awearoners & education activities.

(7) Detaild discription of purpose of the plan.

(8) Contingency plan testing & recovery procedure.

(9) List / name / & / number etc. of vendor for emergency purpose

(10) medical procidure in case of injury

(11) Insurance papers & claim form.

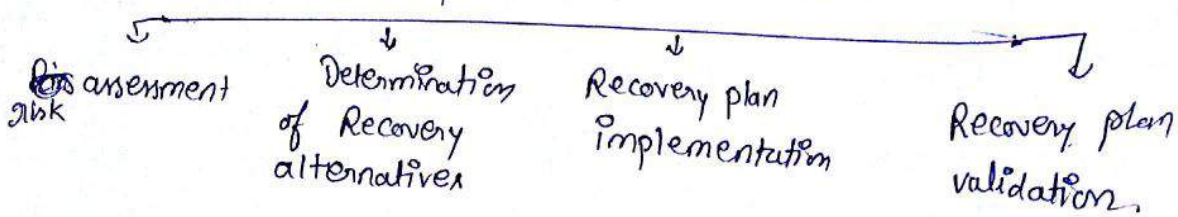
(12) Emergency phone numbers

(13) Name & details of Employees trained for emergency situation.

(14) Backup location etc.

(15) details of air lines, hotels etc.

⇒ Different sections of Busines Recovery life cycle



⇒ objective / goals of Busines Continuity planning :-

1. minimize the damages / Lones from disaster.
2. Reduce the Complexity of Recovery procidure
3. facilitate effactive Co-ordination in Recovery procidure.
4. Provide seafty & well being to the people in premises at the time of disaster.
5. Continue critical busines operation.
6. Establish management Succession & emargency power.
7. minimize the duration of Recovery.
8. Primery objective of BCP is to enable orgnization to Survive a disaster & reestablish normal busines operation.

⇒ Busines Continuity management (BCM)

it is management procces of enterprise to manage all kind of disaster/disruption & providing all kind of Counter measures to Safguard from the insident of disasters.

BCP is a part of BCM

CH-5

→ Reasons why Org. fails to achive their System development objectives imp

→ I SLAP NEW TECHNOLOGY DEVELOPMENT

1. Inadequate Testing & user training.
2. Shifting user needs.
3. Lack of Senior management Support & involvement in info. System development
4. Lack of Participation.
5. New technology
6. Development of Strategic System

⇒ Fact finding techniques:

Every System is build to meet some needs, Say Cost reduction, better Performance etc. To access these needs, the analysts often interact extensively with the people, who are to be benefitted with the System, in order to determing what their actual requirements are.

↓

I DO OBSERVATION

Interview, Documents, Observations, Questoning.

⇒ Functional area of present System, that needs to be annalysted to investigat present system.

investigation of present System involves, Collecting facts, orgnizing facts & Evaluation of the facts about the System & the Environment in which it operates. → methods are → $R^2R^2A^2$

↓

① Review of historical aspects.
② Review of file maintained.
③ Review of method, procedures & data Communication
④ Review of Internal Control.
⑤ Analyze output.
⑥ Analyze inputs.

⇒ System Implementation Conversion Strategies :- there are diff. Strategies.

① Direct implementation / About Change-over :-
Completely shifting from old system to new on a set date in one go.

② Phased implementation :- Some files are converted into new & others files continue in old & slowly stage by stage Conversion

③ Pilot implementation :- one whole operation is replaced with new but only one small operation or only at one branch etc. & then after detecting & eliminating foudal probs. replicate throughout the whole System.

④ Parallel Running implementation :- New & old. Both are used allong side & once new is all set, Stop old.

⇒ Activities involved in Conversion :- System Scheduling FS procedure schedu
① Procedure Conversion. 3rd
② File Conversion - 1st long before programming & testing is Completed
③ System Conversion - 2nd
④ Scheduling personnel & equipment 4th

⇒ Activities involved in implementation Stage

(1) Procurement of Equipment. i.e necessary hardwares etc,
(2) Site preperation i.e find the place which provides required humidity temprature etc for intalled Equipment
(3) installation of new hardware/Software.
(4) Equipment checkout.
(5) Training personnels.

for feasibility - Technical feasibility, Economical feasibility, & operation feasibility.

⇒ Post implementation Review: I DO

IMP (1) Development Evaluation: Evaluation of development process to check whether System was developed on scheduled time & within Scheduled Budget.

(2) operation evaluation: To check if hardware & Software are Capable to perform their duties.

(3) Information Evaluation: this is difficult & Can not be Conducted on a quantitative manner. the objective of Information System is to provide information to support the org. decision making. ∴ the extent to which info. poovided by the System is supportive to decision making is the area of Concern in evaluating the System.

⇒ System maintenance:
It is an important aspact of System development life cycle (SDLC)
A programmer spat more time on maintaing the software then on writing it. the need for modification arrives when/from failuers to anticipate the all requirments.

imp
Types of System maintenance :- See. 138 RF

(1) Scheduled maintenance :- pre planed precautions.

(2) Rescue maintenance :- not anticipated & requires immidiate solution.

(3) Corrective maintenance :- This deals with fixing bugs with in code or defects found. that could be ~~destroing~~ designing error, logical error etc.

(4) Adaptive maintenance :- This consists of adapting software to change in the continious changing environment.

(5) Perfactive maintenance :- accomodating new & changed user requirment.

(6) Preventive maintenance.

v. imp
⇒ System Development Methodology :-

it is a - (1) formalized
(2) Standardized
(3) well orgnized, &
(4) Documented set of activities → which is used to manage a system development project.

This refers to a framework that is used to, structure, to plan & to control the process of developing an information system.

→ methodology of system development are :-

(1) The project is divided into number of identifiable process, & each process has starting & ending point.

(2) Specific reports & other documents (called deliverables) must be produced periodically during the development of System, to make personnel accountable for faithfull execution of their task in developing the System.

(3) User, manager, auditor/Accountant should participate in the project & test for Completability, Cost benefits, Control etc.

(4) System must be tested throughout by implementation

(5) A training plan is developed for those who are going to use new system.

(6) Changes if any should be made through a formal program controls & unauthorized changes in Computer should not be allowed.

(7) A post implementation review of all development System must be performed.

⇒ Approaches to System Development :

Since the orgnizations varies in the way that, they automate their business procedures, & Since each new type of System differs from from each other, Different System development approaches are often used within an orgnization.

- Types of Stytem Development / SDLC approaches

① Waterfall / Phase wise development / Traditional approach or Sequential approach.

② Proto typing / prototype model :→ i.e developed for a small/part of system it is a small version & if sucessfull then real system is developed.

③ Incremental model → adding till more every time.

④ Spiral model ↳ it contains both waterfall & Prototype.

⑤ Repid application development. ↳ which uses minimal planning in favour of rapid prototyping

⑥ Agile methodology.

→ 4 Steps in prototype

① Identify information system requirment
② Derelope initial prototype
③ Test & Review. & Revise
④ obtain user signoff on the approved prototype.

→ SDLC involves various steps in a sequence to develop a computer based information system for an org. the main goal is to improve the existing performance through better procedure & methods.

↓

Stages of SDLC

↓

1. Preliminary investigation.
2. System analysis @ Requirment analysis.
3. Design the System
4. ~~Acquisition &~~ development of software.
5. System testing
6. Implementation.
7. maintenence.

⇒ System Development tools:

1. System Components & flows:- this helps the analysts to document the flow of various activities & flow of various resources used in Information System.
2. users Interface:- Designing an interface b/w end users & Computer System is a major Consideration of System analyst while designing new System.

③ Data attributes & relationship :-

Data resources used in info. System are defined, ~~entered~~ catalogued & designed by this tool.

④ detailed System proces :-

⇒ Data Dictionary :- it is a Computer file which stores discription of all data element their attribute, & relationship

it Contains

① name of Computer file.
② name Computer programs that modify data
③ users allowed
④ user not allowed
⑤ Programs allowed
⑥ Programs not allowed
⑦ Source document etc

& hence helps in

① auditor as a guide.
② helps in audit trial.
③ helps in planning the data flow.
④ serves as aid in investigation & developing Internal Control procedure.

⇒ Validation of vendor's proposals

i.e Contracts & Software licencing. proces

it Consits of evaluating & ranking the proposals submitted by vendors. & ~~is quite difficult~~

these are quite expencive & time Consuming, But has to be done, no option.

- The followings are considered while evaluation & selection.

① Performance Capacity in relation to its Cost
② Benefits from it in relation to Cost
③ maintainebility of it
④ Compatibility of it with existing System.
⑤ & vendor's Support.

→ validation methods of proposal]

① Point Scoring Analysis
② Check lists.
③ Public Evaluation.

Public - check - point

→ Program Debugging : it is a methodical process of finding & reducing, the number of, bugs or defects in a Computer program thus making the Computer behave as it is expected to.

Steps

① Inputting the Source program into the Compiler.
② Letting the Compiler find the errors in program.
③ Correcting the lines of Code that has errors &
④ Resubmitting the Corrected Source program as input into Compiler

⇒ System testing :-

It is a process of identifying (Evaluating) the Correctness, Completness & quality of a DEVELOPED computer software.

Testings should, Systematically uncover the different class of error with minimum amount of time & efforts.

- Data Collected by testing provides reliability & quality of Software.

Types

(1) unit testing :- ~~testing of Source Code~~

testing if individual units of Source Code are fit to use.

there are 5 Catagory of tests that a programmer typically performs on a program unit.

Here are not type of UTP

(a) Functional Tests :- Check if Programs Do what they are Suppose to Do.

(b) Performance tests :- to check Responce time & Execution time, Through put, Primery & Secondary memory usage, Traffic Rate on Data channel & Communication Link

(c) Stress testing :- test to check the stability of a given System it involves testing beyond normal operation Capacity of System.

(d) Structural tests :- testing the internal processing logic of Software

(e) Parallel test :- Same tests are used in new & old system & then output are Compared.

→ Types of unit test program

① Static testing:- here you have a checklist to check whether the work you are doing is going in accordance with the set standards of the organization

② Dynamic testing:- here we give input value & check if the output is as expected.

ⓐ Black box ⓑ White box ⓒ gray box.

⇒ Regression testing :-

it is done to ensure that unmodified part of the program modules are intact, i.e. Changes made in one place should not have impact on other place.

⇒ ~~System testing : Overall~~

⇒ System testing is an overall testing of software & other element as a whole.

↓

Types

↓

Recovery testing :- How well the application will be able to recover from System failure, hardware crash etc.

Security testing :- to determine the security of data, etc.

Stress & volume testing :- Same as stated before.

performance testing — " —

⇒ Final Application testing :-

It is conducted right by the implementation of System to ensure quality & user's satisfaction.

↓

types

(1) Quality Assurance testing :- to check new system satisfies the quality standards.

(2) User Acceptance testing :- to ensure the same.

↓

2 types.

(1) Alpha testing :-
↓
testing within the org.

(2) Beta testing
↓
sending out to test.

⇒ Advantages of SDLC to IS auditor :

(1) IS auditor will have clear idea & understanding of various Phases of the SDLC on the basis of detailed documentation created during each SDLC phase.

(2) IS auditor on the bases of his examination, can state in his report about Compliance is mgt. with the procedure, if any set by mgt.

(3) It will provide guidance to IS auditor.

⇒ factors influencing the org. towards Control & audit of Computers :-

① Cost of Computer abuse - i.e unauthorize access.
② High Cost of Computer Errors :-
③ maintenance of privecy.
④ Cost of incorrect decision making.
⑤ Org. Cost of data loss.
⑥ System Effectiveness objective & efficiency.
⑦ Data integrity objective.
⑧ Assets safeguarding objective.

⇒ function of IS Auditor :- to make Sound Assesment of Risk related to
① Inadequate information Security Control
② Inefficient use of resources.
③ Inefficient Info. technology Stratagies, policies, & practice
④ Info. technology - frauds.

⇒ Catagories of Audit :- ~~SISTM~~ SPITD

① System & application :- To ~~ensure~~ verify the appropriatness of System & adequately Controled to ensure validity, Reliability, timelyness & Security/input Secured input, processing & output at all level of System activity.

② Information processing ~~activity~~ facility :- To ~~ensure~~ verify the processing ~~unit~~ facility is under control. to ensure ~~that~~ timelyness, accuricy & efficient processing ~~of processing~~ of application.

③ System development :- To verify that the System which is under development, meets objectives of org. & ensure that the System is developed in generally accepted standards.

④ Management of Info. tech. & Enterprise Architecture :-
An audit to ~~ensure~~ & verify that IT mgt. has developed an organizational Structure & procedure to ensure a Controlled & efficient environment for info. processing.

⑤ Telecommunications, Internets & Externets :- An Audit to verify that Control are in place on the client - Serve & on the network connecting the client's & Server.

⇒ Steps in IS Audit :-

① Scoping & pre-audit survey :- Determine the Scope of audit & areas out-of-Scope of audit, by the term with mgt. to collect information at this Stage - Source are -> Background reading, web browsing, Previous audit report etc

② Planning & preperation :- Based on ① - plan audit.

③ Fieldwork :- Gathering info. by interviewing staff, reviewing documents etc.

④ Analysis :- Reviewing & trying to make Sence of the information gathered.

⑤ Reporting :- Reporting to mgt.

⑥ Clouser :- it involves preparing notes for future audit & follow up with mgt. to Complete the actions from their end.

→ Concurrent audit :

In on-line processing system, data preparation & processing function take place simultaneously. Therefore, transaction processing may take place without leaving a satisfactory audit trial. In such a case, evidence gathered after data processing is not satisfactory. In order to overcame this a continious audit is carried out.

↓

Type of Concurrent audit

↓

(1) Snapshot technique
(2) Integrated test facility technique (ITF)
(3) System Control audit review file. (SCARF)
(4) Continious & Intermittent Simulation. (C.I.S)
(5) Audit hook

↓

(1) Snapshot : Tracing of transaction in computerized system can be performed with the help of Snapshot or extended records. The Snapshot software is built into the system at those points where material processing occures, which takes images of the flow of the transaction as it moves through the application. The image can be utilized to assess the authenticity & accuracy & Completeness of the process carried on the transaction.

(2) I.T.F. :- To verify the processing authenticity, accuracy & Completeness A dummy entity is created into application system file, & the processing of audit test data would be carried out. Such test data will be included into the normal production data

used as input of processing System.
In such case, auditor has to decide the method to be used to enter the test data & the method for removal of the effect of Dummy transaction.

③ SCARF: System Control audit review file uses embedded audit modules to Continiously monitor transactions activity & Collect data on transactions for audit purpose. Such data are recorded in SCARFile. The transactions that are recorded includes those, that exceed specific limit. say amount etc. Periodically auditor review the data Collected in SCARF.

④ CIS: it embeds (fixes) an audit module in a data base. The CIS module examines all transactions that updates the database using SCARFile.
If a transaction has special audit significance, then CIS module process the data independently. Records the Results & Compare them with those results from database, if discripency is found, CIF may prevent the database from executing the update process. & investigation can be made to identify the reasons.

⑤ Audit hook: there are audit routines that flag Suspicious transaction. Audit hook is used to tag the records with name / address change. the Internal audit department will investigate these tagged transaction records for detecting frauds. questionable transactions will be informed as soon as the occurs

⇒ By using SCARF auditor might collect following

① System ~~Expectation~~ exceptions.
② Policy & procedure variance
③ Application system errors.
④ Performance measurment
⑤ Snapshots & extended record.

⇒ Audit trial:

Audit trial can be designed to Record the activityies. Audit ~~trial~~ acts as an important tool in detacting any errors, frauds etc. The audit trial will ~~have~~ one logs to Collect the event with a sequence.

→ objective of audit trial are:
① Detecting unauthorized access to the system.
② facilitating the reconstruction of event, &
③ Promoting personal accountability.

⇒ Operating System Controls:-

Operating System ~~provides~~ is a Computer Controlled program (not application). it provides interface b/w Computer & user. It allocates ~~the~~ or manage the usage of ~~the~~ Computer Resources (ie CPU, etc.) to the users / applications.

Various tasks performed by ~~app~~ operating System Control.
① Scheduling job sequence in which they are to be performed.
② Managing hardware & Software Resources: they make first, the users application program to be exicuted first by loading them into primery storage & then cause the various hardware units to perform ~~the~~ their specified tasks.

③ Maintaining Security by providing facility of user login passwords etc

④ Enabling multiple user Resource sharing.

⑤ Handling Interruption: i.e. temporarily suspending the processing of one program in order to allow another program to be executed.

⑥ Maintaining Usage records.

⇒ objective of operating System:

① Control objective:

i) Protect itself from user.
ii) Protect user from each other
iii) Operating System must be protected from itself.
iv) " " from environment.

② objective of operating System Security:-

following Security Components

(i) Login procedure - passwords etc

(ii) Access Token:- after successfully Loging in → operating System Creates an access token, that Contains key info. of user. including userid & password.

(iii) Discretionary Access Control: giving access to a particular part of system. & allowing them to use their related area.

③ Remedy from destructive program:- i.e take precaution to protect distruction - use antivirus, purchase from reputed vendor. etc.

⇒ Data management Control

① Access Control ② Backup Control.

⇒ System development Control : Controls targeted to ensure that proper documentation & authorization are available for each phase of the system development process.

↓ Six activities

① System Authorization Activity : To ensure All new system request must be formal (i.e in writing) & duly authorized, by submitting to professional who will develope the system. To ensure that economic & other feasibility are evaluated.

② User evaluation Activity : User must be actively involved in the system development process. User involvement should not be ignored because of a high degree of technical complexity in system. A user specification document should be created by the joint efforts of the user & system professional. This document remains a statement of user needs.

③ Technical design activity : The technical design activity in the SDLC translate the user specifications into a set of detailed technical specification of a system that meets the user's need.

The adequacy of these activity is measured by the quality of the documentation that emerges from each phase.

④ Program testing : All program must be throughly tested by implementation

⑤ User test & acceptance procedure

⑥ Internal auditor's participation

⇒ Source document Control:-

In System that uses physical source documents, to initiate transaction, careful control must be exercised over these instrument. Source document fraud can be used to remove assets from eg. To Control such frauds 7 followings to be taken care

(1) use pre-numbered source document → if any manupulation with source document happens, in audit, that can be easily traced.

(2) use source document in a sequence i.e issue sale bills etc in sequence to keep proper record.

(3) Priodically audit & reconcile the source documents.

⇒ Data Coding Controls: two type of Error that can happen & that can corrupt data code & cause processing error :-

(1) Transaction Error: 3 classes

i) Addition Error: i.e Extra digit or character is added to the code. e.g. instead of 8123 → puted → 81234

Truncation → ii) when digit is removed from end code i.e 812 instead of 8123

iii) Substitution Error i.e putting 8122 instead of 8123

(2) ~~Transportation~~ transposition Error:

(i) Single transportation Error when two adjacent digits are reversed i.e 124568 instead of 125468.

(ii) multiple transportation error when non-adjacent digits are transposed i.e 128956 instead of 248789

⇒ Validation Controls:-

Input validation Controls are intended to detect errors in the transaction data before the data are processed → 3 level of input validation

(1) Field interrogation:- It is a programmed procedure that examine the characters of data in the field:- various field checks.

i) Limit check:- i.e to ensure no errors exceeding a limit.

ii) Picture check:-

iii) valid code check.

(2) Arithmetic check.

(3) Cross check.

⇒ Various process Control:-

(1) Run-to-Run totals:- todays total (1st Jan) ± total of of 10 day = should be equal to ending of 11th Jan.

(2) Reasonableness verification:- two or more fileds are Compared to verify the Correctness.

Ex:- total of depn. of all assets add & also gross depn call culated to cross check the accuracy

(3) Edit check :- to verify Completnes of data.

(4) Field Initialization:-

(5) Exception report:- give details why particular data should not be processed.

CH-8

⇒ **Cloud Computing**: Cloud Computing simply means, the use of Computing Resources as a Service through network, typically the internet. Internet is commonly visualized as cloud. hence Cloud Computing is done through internet. user can access their data-base using internet from any where without worrying about any maintenance or management of actual resources. Beside this, cloud is highly dynamic & scalable. In fact, it is very independent platform in terms of Computing. best Ex. of cloud is. Google 'Apps, where any app. can be accessed using browser & it can be deployed on thousands of Computer through internet.

⇒ **Objectives of cloud**

(1) To Create a highly efficient IT ecosystem, where resources are Pooled together & Costs are aligned with what resources are actually used. (i.e with the actual usage of resources).

(2) To access service & data from anywhere & anytime.

(3) To scale the IT ecosystem quickly, easily & Cost-efficiently; based on the evolving business needs.

(4) To Consolidate IT infrastructure into a more integrated & managable environment

(5) To reduce Cost related to IT energy/power Consumption.

(6) To enable/improve Anywhere access for increasing users &

(7) To enable rapidly provision of resources as needed.

Characteristics of Cloud Computing: Read/Rj (204)

(1) Maintenance: Cloud Computing is easier, as they need not be installed on each user's Computer & Can be accessed from diff. places.

(2) Agility: It shares resources amongst user responsiveness.

(3) High Scalability: Cloud environment enables servicing to business requirment of lazy audiance.

(4) High availability & reliability: Availability of servers is high & are more reliable, as the chance of infrastructure failure is minimal.

(5) Service in pay-per-use mode: Pay for ~~use~~ Howmuch you used.

(6) Virtualization: this technology allows ~~user~~ server & storage devices to increasingly share & utilize the apps, by easy migration from one physical server to another.

(7) Performance: it is monitored, Consistent & loosly coupled architecture are constructed using web services as the system ~~info~~ interface.

(8) multy ~~user~~ sharing.

⇒ Advantages of Cloud Computing:

(1) Cost efficient
(2) Almost unlimited storage Capacity
(3) Ease in Backup & Recovery.
(4) Automatic Software integration.
(5) Easy access to information.
(6) Quick deployment.

⇒ Challanges/ disadvantages of cloud:-

(1) Confidentiality :- Prevention of unauthorized ~~disclosure~~ disclosure of data is referred as Confidentiality. & cloud is bescally works on public network. ∴ to keep data Confidential is a Challanging task. But by encripting & physical Isolation data can be kept confidential. So to keep secrecy - Encript the data b4 putting in cloud.

(2) Integrity :- it refers to prevention from unauthorized modification into the data & ensure that data is high quality, correct, Consistent & accessable. So the main prob. is, after moving the data to cloud, the owner is always worried abt integrity of data.

(3) Availibility :- it refers to prevention from unauthorized holding (or) withholding of data & it ensure the data backup through Business Continuity planning (BCP) & Disaster recovery planning. etc. So the prob. here is of temprorary breakdown, sustained & parmanent outages ; Denial of service attack, equipmet failuer etc. which could effect the availability.

(4) Governance :- Due to lack of Control over the employees & services, it creates problems relating to design, implementations, testing & deployment.

(5) Trust :- various client's oriented studies has revealed that Clould has faild to built ~~doust~~ trust b/w client & service provider. Trust to ensure various service arrangement & visibility of security, privecy control, etc.

(6) Privacy :- Cloud should be designed in such a way that it should decrease the privecy risk.

(7) Data stealing.

⇒ Perfaulment issues in cloud Computing: HITS

① Threshold policy :- it is of an 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 & results in the creation of addition instances of VM in the demand.

② ~~interoperability~~ Interportebility :- if Co. creat application with one Cloud Computing vendor, the Co. may find it difficult to change to another Computing vendor that has different formats for importing & exporting data. This may creat a prob. of achiving Interportability of appl. b/w two Cloud Computing vendor.

③ Hidden Costs :- Like any such Services, cloud Computing will also have hidden Costs.

④ Security issues :- instead of waiting for outraged damages, check by yourself, how long the cloud vendor take to recover the data in case of any emergency.

⇒ Cloud v/s Grid Computing :-

Cloud Computing is evolved from Grid Computing only. Cloud provides on-demand resources. Grid Computing, may, or may not be their in Cloud, depending upon users using it. if user is System administrator / & integrators, they care, how things are maintained in cloud.

Grid Computing requires the use of software that can divide & Carve out in pices of a program from one large image to serve thousand Computer.
one Concer about grid is that if one pice of software on notde fails another pices of software on other node may fail.

⇒ Cloud Computing Architecture (CCA):
~~It is a cloud~~ CCA of a cloud solution is a structure of System which contains on-premises, cloud resources, middleware & services & software Components, their geo-location & their externally visible properties & the relationship b/w them.
Cloud Architecture typically involves into multiple cloud Component Communicating with each other.
A Cloud Computing Architecture ~~Composes~~ Consists of

(1) front end Architecture :- The front end of cloud Computing System, Composes of the clients device & some applications needed for accessing the cloud Computing system.

(2) Back end Architecture :- Back end refers to some Service facilitating phampherals. In cloud Computing, the back end is Cloud itself.

⇒ Cloud Computing Environment : Can Consists of multiple type of clouds, based on their developments & usage. Such Cloud Computing environments creating to special requirment are:-
(a) Types of Cloud Computing are:- (a) Pvt. cloud. (b) Public Cloud.
(c) Community Cloud (d) Hybrid Cloud

(1) Public Cloud: this are such type of service which is available to any subscriber, with an internet connection. The capital expenditure is almost nil. & it is not restricted to any org.

(2) Pvt. Cloud:- Pvt. cloud is restricted to any particular orgnization. it is suitable for MNC's & those org. which have huge budget for IT. This is primerily developed by Co.'s IT department.

(3) Community Cloud:- Community cloud shares infrastructure b/w several org.s. from a spacific community with common concern (security, Govt etc.) whether managed internally or by third party hosted internally @ Externally

(4) Hybrid Cloud:- It is a combination of two @ more types of cloud models. Say atleast one pvt. & 1 public cloud computing where in pvt. cloud (Existing) will enter into partnership with public cloud provider. @ vice-versa.

⇒ Various cloud Computing models

(1) Infrastructure as a Service (IaaS):- IaaS providers provide the infrastructure/storage required to host the service by the cloud client. Here cloud client become the system administrator & manage hardware/software, network & computing resources.
In order to deploy their apps. cloud client install operating system & their apps software on cloud infrastructure
Ex:- DNS, Google Compute Engine, HP cloud etc.

(2) Platform as a Service (PaaS):- provider will provide platform App. developer can develop & run their software solution on a cloud without cost & complexity of acquiring & maintaining H/w. & S/w

(3) Software as Service (SaaS):- Provider will provide large verity of apps. over Internet, hosted on their infrastructure, & user can use them. Ex:- google doc. online, pixlr.com. etc.

(4) Network as a Service (NaaS):- It is a category of cloud service where the capability provided to the cloud service users to use Network Connecting services:- Ex:- VPN & mobile network etc

(5) Communication as a Service (Caas):- It is an outsourced enterprise Communication Solution, which is obtained on lease from a single vendor, & the vendor is responsible for H/w & S/w maintenance & offers guaranteed Quality of Service (QoS) it allows businesses to selectively deploy Communication devices & modes on a pay-as-go basis.

=> Mobile Computing :- it refers to the technology that provides/allows transmission of data via a Computer, without having to be connected with a fixed link. (physical link.)

* It enables, mobile sales personnel to update work order status in real time, facilitating excellent Communication.
* It facilitate corporate service & info. at any time & from any place.
* It provides remote access to corporate knowledge at the Job location..
* it enables to improve mgt. efficiency by enhancing info. quality, info. flow, & ability to control a mobile network.

⇒ Bring your own Device (BYOD)

it refers to a business policy that allows the employees to use their own devices viz Smartphone, Laptops etc. for the business purposes. & employees are welcomed to Connect their devices to Corporate network, to access info. & application.

Risks in BYOD:

(1) Network Risk:- if Org's own devices are their then IT people will know, how many devices are Connected to network & they will know the flow of data from network. But if BYOD then they will not be able to know which all devices are connected to network & is suppose in case if virus hit the Network, they may have to Scan whole the devices & in this process they might miss out Scanning Some of the devices.

(2) Device Risk:- the Device of employee which is used under BYOD if lost then it may Create a huge prob. of Repo & Confidential info. of Co.

(3) Implementation Risk:- the effective Implementation of BYOD program should not only Cover the technical issues but also madate the development policies.

⇒ Web (or) web 2.0:- The term is given to define 2nd generation of world wide web, that is focused on the ability for people to collaborate & share info. online.

web. 2.0 is bessically refferes to transition from HTML to a more dynamic web that is more organized & is based on Serving web applications to users.

Major Components of web 2.0 : It includes the following features.

(1) Communication :- these are groups of individuals to share thoughts, ideas & variety of tools to promot social networking.

(2) Blogging :- Blogs ~~are the~~ gives the freedom to the users of Social Network to express their thoughts in a free form basis & help in generation & discussion of topics.

(3) Wikis :- Wiki is a set of co-related pages -> on a particular subject & allowes the user to share Contents. wiki replace the complex document management system & are very easy to create & maintain.

(4) Folksonomy :- web 2.0 being people-centric technology has introduced the feature of ~~fol~~ folksonomy, where the user can tag their Contents online & this enables others to easily find & view others Contents.

(5) File sharing / podcasting :- This is the facility, which helps users to send their media files & related Contents online for others people of the network to see & contribute.

(6) Mashups :- This is the facility, by using which, people on the internet can Collaborate services from ~~many~~ multiple vendors to create a completely new service. An example is - Combining the location info. ~~of~~ of mobile service Provider & the map facility of google map, in order to find the exact info. of cell phones location from internet, by just entering the cell phone number.

=> Social media :- it is created by a group of few individual who have a set of Common interests & objectives. they are usually a set of network formators followed by a broadcast to achive network membership. this happens both public & pvt. groups depending on Confidentiality.