Page No.
Date: / /201

* Waterfall Model:

- The waterfall Model is a Traditional development Approach in which each developer works in different phases.
- In traditional approach of systems development, activities are performed in sequence
- Unless earlier step is completed, Next step is Not undertaken under traditional approach.

Characteristics:

1) divided in to sequential phases — Project is divided into sequential phases, with some overlap and splash back acceptable between the phases.
2) Emphasis on planning — Emphasis is on planning, time scheduling, target dates, Budgets and implementation of an entire sys. at one time.
3) Tight control — Tight control is maintained over the life of project through extensive use of written documentation.

Stronghts: [COMIC]

1) Conserves resources
2) An orderly sequence of development steps and design ensures the quality, reliability etc of the developed sof
3) Progress of systems development is Measurable
4) Ideal for less experianced project teams or where a composition Team fluctuates.

Weakness: [SPLIT-FC]

1) It is slow, costly and combersome due to tight controls. maintained ov
2) Problem can't be discovered due to lack of sys. testing
3) Depends upon early identification and specification requirement from users which users may not able to clearl defi
4) Excessive documentation at each stage is time-consumi and also difficult for the users to read it regularly.
5) Project progresses Forward with little scope for backward
6) Difficult to respond to changes. changes occurring later in the system are more costly and hence discourage

Page No.
Date: / /201

* Prototyping Model:

⇒ • The goal of prototyping approach is to develop a small or pilot version of a system called prototype.
• A prototype is built quickly at lesser cost and with the intention of being modifying or replacing it.
• As users work with the prototype, they make suggestions for improvements which are then incorporated and finally a prototype satisfying all the users requirement which is either turned into the final system or it is not suitable, it is scrapped.

☞ **Strenghts:**

1) Improve user participation in sys. development.
2) Easily identify confusing or difficult functions and missing functionality.
3) provides quick implementation of incomplete, but functional application.
4) Knowledge gained in an earlier iteration is used in development of later iterations.
5) Encourages innovation and flexible designs.
6) A very short time period is required to develop and start experimenting with a prototype.
7) System more reliable and less costly to develop.

☞ **Weakness:**

1) Lack of the user strict control for sys. development.
2) Frequently changes in Requirement may cause delay and over cost for the system.
3) Some time developers are unable to meet the requirement in actual system as shown in the prototype to users, which may cause dissatisfication in the system user during actual use.

Page No.
Date: / /201

4) It can be successful only when the sys. developers are ready for providing significant time to experiment and build prototype & get it checked from Actual user again & again untill user APPROVES the prototype.

* Info. P.F = Information processing facilities.

Page No.
Date: / /201

XREX 3.29

MTP M.15

* Points for Audit of Environment control that Auditor would consider while conducting Audit?

⇒ 1) Water Detector: The presence of water Detector are verified on visiting Computer Room
2) Hand Held Fire Extinguisher: The presence of Fire Ext. at strategic location throughout the facility are ch
3) Manual Fire Alarms:
4) Smoke Detectors: Presence are verified on visiting computer Room
5) Fire Suppression System:
6) Water - based systems
7) Halon system
8) Fire proof walls, Floors & ceilings Surrounding the com. R
9) Uninterruptible Power Sys. (UPS) / Generator
10) Power Leads Two Substations: Auditor check whether the Info. P. has extra power connection for emergency power off situation
11) Electrical surge protectors: Presence of electrical surge protect for sensitive & expensive computer
12) Emergency Power-off switch
13) Fire Resistant Office Materials.
14) Documented & Tested Emergency Evacuation Plans.
15) Wiring should be placed in Electrical panels

1011 * Governance of Enterprise IT (GEIT)

⇒ • GEIT is a Sub-set of Corporate Governance AND Facilitates Implementation of a Framwork of IS Controls within enterprise as relevent & encompassing All Key Areas.

• The primary objectives of GEIT are to Analyze and articulate the requirements for the (GEIT) Governance of Enterprise IT, and to Implement and maintain effective enabling Structure with Clarity of responsibilities & Authority to achieve the enterprises's missin, goals & objectives.

Benefit of GEIT

1) It provides a consistent approach which integrated and aligned with enterprise Governance approach.
2) It ensure that IT-related decisions are made in Accordance with the enterprise's Strategies & objec
3) It ensure that IT-related process are overseen effectively & transparently.
4) It ensure that the governance requirements for Board members are met.
5) It confirms compliance with legal & Regulatory Require

RTPM-15 Pg. 30 * COBIT & its Components

⇒ • COBIT is a Set of Best Practices for I.T. Management develop by ISACA AND IT Governance Institute in 1996.
• COBIT is a framwork which provides Audit Guidelines
⇒ Audit Guidelines / Standared For Auditor
⇒ Control Procedure & Benchmarks For Management.
⇒ and Assurance Procedure For User.
• In general COBIT Help organization to achive Busines ob
Component of COBIT: 1) Framework 2) Process Discription 3) Control objectives 4) Management Guid lines 5) Maturity Models

FP
CMM

2.11 * Characteristic of CBIS.

Predetermined objectives 1) All sys. work for predetermined objectives and therefore designed and developed accordingly.

Depends on other subsys. 2) Sys. has Number of Interrelated & Interdependent Subsystem. It depends on other subsystems for its inputs

Sys. fails 3) If one subsys. or component of a sys. Fails. The whole sys. does not work.

Interact 4) All sub-systems Interact with each other in such a way that they work to achieve the goal of a system

Integrated 5) The work done by individual subsystems is integrated to achieve the central goal of the system

* MIS ⇒ MIS has been defined by Davis & Olson as
- "An Integrated users-Machine system
- Designed for providing Information
- To support operational control, Management control and D.M. functions in an organization."

RTP W.14 2.16 N.12 MTP M.15 CII * EIS ⇒ or ESS ⇒ EIS used to provide Info. to TOP Management.

Characteristics:

1) EIS is CBIS that serves the info. to TOP Management.

User friendly 2) very user friendly

Rapid Access 3) EIS provide Rapid access to timely Info.

Online analysis tool 4) EIS provide extensive online analysis tool

Drill down 5) EIS provide Drill down Reporting

Internal & External 6) EIS is capable of accessing Both Internal & External Data.

7) It locates Problem without the need to learn query language

8) EIS can easily be given as a DSS Support for D.M.

RTP M.15 * Discuss the Type of Info. system

Diff. Info. Sys. that serve diff. organizational levels.

1) operation level sys. 2) Knowledge level sys.
3) Management level (Middle) 4) Strategic level sys (→ Senior level)

XRox 2.12

Page No.
Date: / /201

* Office Automation System: Application of the computers to handle Office activities are termed as OAS.

[DDR FCR]
1) Document Capture
2) Document creation
3) Recipts and Distribution
4) Filing, Search, Retrieval & Follow up!
5) Calculations
6) Recording Utilisation of Resources

* Benefits of OAS:

Improve Communication 1) Improves communication within ~~the~~ organization & Bet^n enterprise
Reduce cycle time 2) Reduce cycle time Bet^n preparation and Receipt of messages
Reduce cost 3) Reduce cost of office communication
Ensure Accuracy 4) OAS Ensure accuracy of communication flows.

2.14 * MISconceptions about MIS -

⇒ 1) All CBIS is MIS (Computer Based Info. System)
2) All Reporting Sys. is MIS
3) MIS is a Management Technique
4) MIS is a Bunch of Technologies
R 5) MIS is only Related with computers
A 6) Accuracy plays Vital Role in Reporting
M 7) More data means more information to manager
8) MIS is an Implementation of organizational system & procedures.

* ES: • Es is a computerized I.S. that allows Non-Experts to make decision comparable to those of an Expert.
• Es are used for complex & ill structured tasks that require special knowledge in specific area.

MTP M.15 * Discuss I.S. & its components. What are the Activities carried out by I.S. in General.

⇒ I.S ⇒ An I.S. comprises of people, H/S, data, and network for communi. support.

Activities ⇒ 1) Data is collected from an organization or from External environment and converted into suitable formed required for processing (Input)
2) This is converted in to information (More meaningful form) obtained after manipulation of these collected data (processing)
3) Then info. is stored for future use or communicated to user

- This supports DM
- Helps to improve DM
- used for DM
- used to solved semi
- user friendly
- easy to use

- focus
- Flexible & adaptable
- knowledge base

Page No.
Date: / /201

2.16 * What is DSS? characteristics of DSS?

⇒ DSS:- DSS is a system that provides tools to Managers To assist them in sloving semi-structured & Unstructured problems in their own personalized way.

- DSS provide Managers with set of capabilities that enable them to generate the info. required by them to make decisions
- A DSS supports the Human decision-making process, Rather than becoming a means to Replace it.

Characteristics

- 1) This supports decision making & occurs at all levels of mngt.
2) It should be flexible and adaptable
- 3) DSS Focuses on decision Rather than data & Information
4) It should be easy to use. user Need Not to have knowledge of comp.
5) DSS used to slove ~~structured problem~~ semi-structured & Un Structured Problem
6) DSS should be user-friendly.
- ~~7~~) DSS is used Mainly For Decision Making.
- 8) Helps to improve Decision Making.
9) It is a Knowledge base system i.e. allow user to apply his knowledge for prob. solution.

---

* Limitation of MIS? MTPM.15

Quality 1) Quality of output depends upon quality of inputs.

Substitute (Not) 2) MIS cannot substitute the ability of Management For taking decisions. It is only tool

Non Flexible 3) MIS does Not have enough flexibility to update itself with changing needs of management.

Not Tailor made 4) cannot provide Tailor-made packages for every type of prob.

only Quantitative Factors 5) MIS considers only quantitative factors & ignore Non-Quantitative factors.

semi structured Unstructured 6) Do not deals with semi structured or unstructured problems.

Effectiveness 7) MIS effectiveness decreases due to Frequent change in Mngt.

8) MIS Does not provide ad-hoc Reports.

Quality, Quantitative flexibility, Effectiveness Ad-hoc, Tailor made Substitute, semi-structured & Unstructured

TPS ⇒ • At the lowest level of Management, TPS is an I.S. that manipulates data from Business Transaction.
• Any Business activities such as sales, pur., production, payment or Receipts involves transaction and these trans. are to be organ2o & manipulated to generate info.

* TPS Involves ⇒ 1) Capturing data 2) Processing of file/dbase 3) Generating Info. 4) Handling of queries.

2.11 * Principal components of a TPS?

⇒ 1) Input (source docs. used: Journals & Register) 2) Processing 3) Storage (Ledger & Files) 4) Outputs: Any Docs. generated from the sys. is output

2.12 * Features of TPS (N.13) (MTPN.14)

[BALS] ⇒ 1) Large volume of Data 2) Automation of Basic Operations

[LABS] (CLOSH) 3) Benefits are easily Measurable: Helps to reduce workload for Transaction Processing.

4) Source of input for other system: Basic source of internal Info. for other Info. System

* Characteristics of an effective MIS RTPM.12, RTPN.12 N.13

⇒ 1) Management oriented (Info. as per Mgt. requirement, Efficient) 2) Management directed

[CMISCM CC] 3) Integrated (provide output based on integrated functions is considered) 4) Common Data Flows (Not be duplicate data entry, Data entered once should be reflect wherever reqd.) 5) Common dbase (mainly cdbase)

6) Long Term planning (use for long term purpose. It should be adaptable & flexible) 7) Sub system concept

8) Computerized 9) Need based 10) Exception Based

RTPN.14 DM:34 * Constraints in operating a Computer Based MIS

[DELHI] 1) Non-Availability of Experts: who can develop & mange computer Based MIS.

[NNN BP High] 2) Problem of selecting the Sub-Systems of MIS to be Instaleed and operated upon

3) Non-Standardization of MIS: every one can specify their own requirement.

4) High-Turnover of Experts: There is High T.O. Job switching of experts for better Pay-packets, Promotion etc. which cause prob.

5) Non (Lack) Co-operation from Staff

6) Difficulty in quantifying the benefit of MIS.

2.17 * Examples of DSS in Accounting or Accounting Application of DSS

⇒ 1) Cost Accounting system 2) Capital Budgeting System

3) Budget variance Analysis System.

4) General DSS → for W.C Mangement, Ratio Analysis, Receivable Analysis

Book:19 * Components of DSS

[UPMD] 1) Users: user of DSS are known as knowledge based user because they can apply their knowledge for Prob. solution.

2) Planning language: i) General purpose planning language. ii) Special purpose planning language

3) Model Base: • Brain of DSS • M. Base is create with the help of DSS • This provide structure of Prob. to be sloved.

4) Data Base: • Provide input of DSS • Dbase can be user Dbase

• In Large DSS problems the Dbase can be categorized

Three level of Management.

i) External Level (Mange by user & plan lang.) ii) Logical Level (Mange by DBMS) iii) Physical Level (Mange by OS & programmer)

With the help of

* Pre-Requisites of MIS?

⇒ 1) Qualified staff 2) Support the Management 3) Common dbase 4) control & Maintenance of MIS

Page No.
Date: / /201

Book122 * Components of ES [IN U.K.K. Explenation Facility]

1) User Interface: This component provide a user friendly graphical Interface for accepting problems from users.
2) Inference Engine: provides solution of given problem with the help of knowledgebase by applying certain Mathmetical & Statistical rule
3) Knowledge Base: This componey Maintains knowledge of experts For problems solution.
4) Explenation Facility: This componay Format or arrange the solution provided by Inference engine in the user Interface
5) Knowledge Aequisition Facility: This component is used to acquire knowledge of experts and arrange the knowledge in knowledge base in a systematic form.

X Ref 2011 * ~~Attributes of Information~~

Mod-20 * Briefly Describe Five Major characteristics of the

[LOW LEVEL & LACK OF FDI] Types of Information used in Executive Decision Making

1) Lack of Structure (Many decisions taken by executive are unstructured.) 2) High Degree of Uncertainty (Takes decision without having the base of previous Info.) 3) Future orientation 4) Informal Source (Executives rely heavily on Informal source of Info.) 5) Low level of Detail (Decision must be taken by observing broad trends.)

Book115 * Pre-Requisites of a MIS

M.14

1) Database 2) Qualified System and Management staff 3) Support of Top Management 4) Control & Maintenance of MIS (Follow some standards procedures)

2.22 * Attributes of Information [TRMR 2411CH CA CPT Q] VVF

Info. means processed data that have been put into a meaningful and useful context.

1) Timeliness (Availability): very important aspect of Information. Information is useless if it is not available at a time of need.
2) Reliability: Info. should be from reliable sources. It measures failure or success
3) Mode & Format: Mode → voice, text, or combination of both. Format → should be simple, format means
4) Rate: The Rate of Transmission/Reception of information may be represented by the time required to understand a particular situation.
5) Completness & Adequacy
6) Transparency: Info. should be free from any Bicasness.
7) Purpose/Objective: Info. must have purpose at the time it is transmitted to person or machine, otherwise it is simple data.
8) Quality: It means the correctness of Information.
9) Validity: It measures How close the information is to the purpose for which it asserts to serve.
10) Current/Updated: Info. should be refreshed from time to time. Ex: Running score
11) Frequency: The frequency with which info. is transmitted or received affects its value.
12) Value of information: It is defined as diff. Bet the value of the change in decision behavior caused by the information and the cost of the information.

MTP:N14,2 RTPM.15 — Key Governance practice of Risk Management ⇒ Evaluating RM

1) Evaluate Risk Management → continually examine the effect of Risk on current & future use of IT
2) Direct Risk Management → direct the establishment of RM to provide reasonable assurance
3) Monitor Risk Management → monitor the key goal & metrics of RMP

1.12 * **Key Management practices, which are required for aligning IT strategy with enterprise strategy.**

[UADCDC] ⇒
1) Understand enterprise direction: consider the current enterprise environment and business process, as well as enterprise strategy & objective
2) Assess the current environment, capabilities & performance
3) Define the Target IT capabilities.
4) Conduct a gap analysis: Identify the gaps between current & target environment
5) Define the strategic plan and road map
6) Communicate the IT strategy and direction. → To stakeholder & users

1.15 * **Risk Management Strategies** [5T]
1) Tolerate / Accept the Risk (Some Risk are minor → Accepting the Risk as a cost of doing business)
2) Terminate / Eliminate Risk (→ Replacing Tech. with more robust product)
3) Transfer / Share the Risk (→ share with trading partner)
4) Treat / mitigate the Risk (→ suitable controls must be implemented)
5) Turn back: where prob. or impact of Risk is very low, then management may decide to ignore the Risk.

1.16 (Book 2, 56) * **Principles of COBIT-5** [MCA ESe]
1) Meeting stakeholders needs
2) Covering the Enterprise End To End: IS should cover all function & Business Pro.
3) Applying a single integrated framework (→ COBIT-5 helps to align with other required standard)
4) Enabling a Holistic Approach (→ efficient & effective governance & magt. of Enterprise IT require holistic approach taking into account several interacting components.)
5) Separating Governance From Management (° Governance is the responsibility of BOD under leadership chairperson; ° Management is the responsibility of executive magt. under CEO)

1.16 RTP N.14 * MTP N.14 **Key Magt. Practices for Implementing Risk Management** [CA MA DR] MTPM.15-II
1) Collect Data 2) Analyse Risk (→ from collected data, Analyse Risk, taking into account ...) 3) Maintain a Risk Profile
4) Articulate Risk (→ Provide info. on current state of IT-related exposures & opportunities in timely manner) 5) Define a Risk Management Action portfolio (→ reduce Risk to an acceptable level as a portfolio) 6) Respond to Risk: → in a timely manner to reduce the Risk of ...

1.19 RTP N.14 * **Areas, which should be Reviewed by internal Auditors as a part of the review of Governance, Risk and Compliance (GRC)** [~~SGI ERI~~ EBRE]

⇒ Internal Audit Activity must ....
1) Scope 2) Governance 3) Evalute Enterprise Ethics
4) Risk Management 5) Interpretation
6) Risk Management process 7) Evalute Risk Exposures
8) Evalute fraud and fraud Risk
9) Address Adequacy of Risk Management process (RMP)

MTPM.14 * What do you understand by the terms of COBIT ? Describe its Practice in Brief.

→ Cobit -5 Provides key Mngt. Practice for ensuring compliance with external compliances as relevent to enterprise. The practice given as Follows:

[IOC Obtain Assurance]
1) Identify External compliance Requirements.
2) Optimize Response to External Requirements.
3) Confirm External Compliance
4) Obtain Assurance of External Compliance.

Page No.
Date: / /20

RTPN.14 1.2) * Key Management practices for assessing and evaluating the system of Internal control in an enterprise in detail. [MR PIPESE]

→ M 1) Monitor Internal controls → Continuously monitor & improve the control environment to meet org. Objectives.
(N.14) R 2) Review Business process controls Effectiveness
P 3) Perform control Self Assessments: To evaluate the completeness and effectiveness of Mngt's control over process, Policies & Controls
I 4) Identify and Report control Deficiencies.
E 5) Ensure that Assurance providers are Independent & qualified
P 6) Plan Assurance Initiatives Based on enterprise objective, Assurance objective & Strategic Priorities. 7) Scope Assurance Initiatives Baseline & agree with mngt on the scope of assurance inatives.
S
E 8) Execute Assurance Initiatives → Execute planned assurance initiatives. Report on identified findings provide opinions & recommendation for improvement.

MTPM.15 N.13(case) 3.8 * Types of Information Security Polices & their Hierarchy.

→ 1) Information Security Policy 2) User Security Policy
[USA ON CC] 3) Acceptable Usage Policy 4) Organizational ISP
5) Network & System security policy
6) Info. classification Policy 7) condition of Connection

RTPN.14 * Five Interrelated components of Internal Controls [IC RCM]

1) Information and communication
2) Control Environment 3) Risk Assessment
4) Control Activities 5) Monitoring: Elements that ensure IC operates reliably over time

3.13 May14 * Major Financial control Techniques in Brief.

[ABCD IS DSS]
1) Authorization → Transaction are Authorized & only Authorized user are allowed for data entry 2) Budgets 3) Cancellation of Documents → Marks a docx. in such a way to prevent its reuse
4) Documentation 5) Input/output verification 6) Safekeeping
7) Dual control 8) Sequentially Numbered Documents
9) Supervisory Review.

RTPN.14 3.14 * Major Boundary control Techniques in Brief.

[CBIPP]
1) Cryptography 2) Passwords
MTPM.15 3) personal Identification Numbers (PIN)
4) Identification Cards
5) Biometric Devices

Piggybacking: This involves intercepting communication both the OS and the user and modifying them or substituting new msg.

3.16 * Explain Different classifications of Information.

⇒ 1) TOP Secret 2) Highly Confidential 3) Proprietary 4) Internal use only 5) Public Documents.

RTP N.14

3.17 * Major Data Integrity Policies:

N.14 (case) ⇒ 1) virus - signature Updating 2) Software Testing → into Development, Test & Production is required for Critical sys.

[VS DDOS] 3) Division of Environments 4) Offsite Backup Storage 5) Quarter - End and Year-end Backups 6) Disaster Rec.

RTP N.14

3.18 * Explain various Forms of Asynchronous Attacks in Brief.

1) Data Leakage (Critical Resource Forcing) 2) wire - Tapping: This involves spying on info. being transmitted over telecom N/W 3) piggybacking 4) shutting down of computer / denial of service

3.22 * Major Dimensions under which the impact of cyber Computer crime Exposure Frauds on enterprises can be viewed. [FLL DS]

⇒ 1) Financial loss 2) Legal Repercussions

N.14 3) Loss of Credibility or competitive Edge

4) Disclosure of confidential, sensitive or Embarrassing Info.

5) Sabotage: The above situation may lead to misuse of such info. by enemy country. 6) Blackmail

3.23 * Major Techniques to commit cyber frauds

MTP N.14 ⇒ 1) Hacking 2) Cracking 3) Data Diddling (changing data) 4) Data Leakage

5) Denial of service Attack 6) Internet Terrorism

7) Logic time Bombs 8) Masquerading or Impersonation

9) password cracking 10) piggybacking 11) Round Down

12) Scavenging or Dumpster Diving 14) Super zapping

13) Social Engineering Techniques 15) Trap Door

3.22 * Discuss Locks on Doors with Respect to physical Access (control)

⇒ 1) Cipher Locks (2 Diff. means of controlling "PA" control.) 2) Bolting Door Locks (↳ consist push button panel)

3) Electronic Door Locks 4) Biometric Locks.

APR.17 * Impact of Technology on Internal control [PC RAM Se Authorization]

⇒ 1) Personnel (↳ should have proper skill & knowledge to discharge their duties.) 2) Concentration of program & Data (Effect of computer) (↳ Helps to detect Fraud & Errors.)

3) Record keeping 4) Access to assets & Records 5) Mangt. Supervision & Review (↳ maintain Records & control over the protection & storage of Data.)

6) Segregation of Duties 7) Authorization procedures: ensure that Transactions entered are approved by appropriate Authority.

Page No.
Date / /201

5.19 Book:2 Pg.9 → How the Investigation of the Present (Existing) Info. SYS. should be conducted so that it can be further improved upon.

* How the Analysis of present SYS. is made by the SYS. Analyst?

1) Review Historical Aspects 2) Analyze Inputs
3) Review Data Files Maintained 4) Analyze outputs
5) Review Method, Procedures & Data communications.
6) Review Internal controls 7) Modeling the existing Physical SYS. and logical system ⇒ Diff. Diagrams of existing SYS. are prepared in terms of Flowchart, Data Flow Diagram
8) Undertake overall Analysis of present System

5.22 RTP N.14 * Two primary Method, which are used for Analysis of the scope of a project in SDLC.

→ 1) Reviewing Internal Documents
2) Conducting Interviews.

5.23 (N.01, 03) * What are SYS. Development Tools? Major Tools used for SYS.Dev.

→ Tools & Techniques have been develop to improve current information system and to develop new ones. [CID SYSTEM PROCESS]

The Major Tools used for SD can be grouped in four categories.

1) System components & flows (→ helpful to document the data flow among the major resources & Activities) 2) User Interface
3) Data Attributes and Relationships (these very important part of system, phase in IS are define, etc)
4) Detailed system process: These tools are used to help programmer to develop detailed procedure & processes required ~~in the design of a computer program~~

RTP N.14 MTP M.15 Pg: 70 * Major Reasons due to which organizations Fail to achieve their system Development objectives.

⇒ i) User Related Issues:

1) Changing (shifting) user Needs 2) Resistance (प्रतिरोध) To change
3) Lack of user participation 4) Inadequate Testing & User Training

ii) Developer Related Issues:

5) Lack of Standard (S.P.) Project Management and S.D. Methodologies
6) Overworked or Under-Trained Development Staff

iii) Management Related Issues:

7) Lack of Senior Management Support and Involvement
8) Difficult to define the exact Requirements particularly for

5.26 MTP N.14 N.12 * Major characteristics of Good coded Program

⇒ 1) Reliability 2) Robustness (Process of taking input/output in least likely situation) 3) Accuracy

[UAE RRM] 4) Efficiency 5) Usability 6) Maintainability.

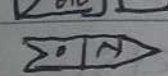
5.27 * Five categories of Tests that a programmer typical

[FPPSS] performs on a program unit (TYPE of Testing)

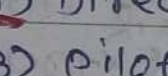
N.13 ⇒ 1) Functional Tests 2) Performance Tests

N.14 case 3) Stress (volume test) Tests 4) Structural Tests 5) Parallel Tests

5.28 * Changeover strategies used for conversion from old to Ne



1) Direct conversion 2) Phased conversion



3) Pilot conversion / Distributed conversion 4) Parallel Con

Dm: 12) N.13 * Various activities that are involved for successful conversion with respect to a computerized Info. System.

⇒ 1) Procedure conversion 2) File conversion

[PFSSA] 3) System conversion 4) Scheduling personnel & equipm

5) Alternative plans in case of equipment failure.

* Feasibility Study:

⇒ 1) Technical 2) Financial 3) Economic (Evaluation of all involved Cost-Benefit Analysis) 4) Operational 5) Behaviour 6) Legal

7) Schedual 8) Resources

also, design by this tools.

* Fact-Finding Techniques: [Doc. Obser I Q]

1) Documents 2) Observation 3) Interviews 4) Questio

* Explain the stages of SDLC [IRDA TIM]

1) Preliminary Investigation 2) Requirement Analysis or Sys.

3) Design of system 4) Acquisition & development of So

5) System Testing 6) Implementation & Maintenance

XROX 5.33 * Types of System Testing: & Discuss Sys. testing?

RIPM.15 1) Recovery testing 2) Security Testing (whether sys. is secured for inputs & outp

[RSS Performance] 3) Stress Testing 4) Performance Testing. (whether sys. can handle required volume & uses.)

2280X620 * Internet & Intranet controls: [what things Auditor should consider while evaluating Internet & Intranet control?]
→ 1) Component Failure
2) Subversive Threats

MTPN.14 N.14 6.25 * Various output control: [EPLS Retention Storage Report]
1) Controls over printing 2) Logging of output Program execution
3) Spooling/Queuing 4) Retention controls 5) Storage & logging of sensitive (Misc) Forms
6) Report distribution & collection controls

6.7. RTPN.14 N.14 * Effects of Computers on Audit: Discuss the issues relating to performance of evidence collection and understanding the Reliability of controls.
→ 1) Data Retention and storage 2) Absence of Input Documents.
[DAN LAL] 3) Non-availability of Audit trail 4) Lack of Availability of output
5) Audit evidence 6) Legal issues.

6.8. MTPN.14 * Major Types of IS Audits or Catagories of IS Audit.
→ 1) Systems and Application (An Auditor verify that SYS & APP are appropriate, efficient, adequate control) 2) Information Processing Facilities
[SISTEM] 3) System Development (verify SYS. under Dev. meet obj. & developed in accordance with generally accepted stand.) 4) Management of IT and Enterprise Architecture: (Ensure controlled & efficient environment for Info. processing)
i. S.A 2. I.P.F 3. S.D 4. TE Mang.
5) Telecommunications, Intranets, and Extranets. (Control place on client server, & Network)

6.9 MTPN.14(2) MTPM.15 * Major stages (Step) of IS Audit in Brief [SPF And Reporting closure]
→ 1) Scoping and Pre-Audit Survey (Plan prepare by dividing scope into areas level wise) 2) Planning & preparation
3) Fieldwork (Gathering evidence by interview, observation, reviewing docs.) 4) Analysis (use of PEST) 5) Reporting (To the mgt. Preparing notes for future ref.) 6) closure.

RTPN.14 6.13 M.13 * Various Types of Information collected by using SCARF
→ Auditor might use SCARF to collect the following types of information:
[ASSSP] 1) Application System Errors: Provide an independent check on the quality of SYS processing.
2) Policy and procedural variances: (Organization have to adhere to the policy, procedure & SOP.)
3) System Exception (can be used to monitor diff. types of app. sys. exe.) 4) Statistical sample
5) Snapshots and Extended Records: (Record can be written into the SCRAF file & printed when required)
6) Profiling Data (To collect data to build profiles of SYS users.) 7) Performance Measurement

RTPN.12 6.13 M.14 MTPN.14 * Advantages of Continuous Audit Techniques
→ 1) Timely Audit 2) comprehensive & Detailed Auditing
3) Surprise test capability 4) Information to system staff on Meeting of Objectives 5) Training for New users.

RTPM.12 6.14 M.14 * Disadvantages of Continuous Audit Techniques.
Require Expert Knowledge → 1) Require expert knowledge of Audit Software used and client SYS. working from Auditor.
Availability of Resources 2) Availability of Resources, like, Audit Modules and online SYS. facilities. (Auditor should be able to obtain resources required from the organization)
Involvment in SYS. Dev. 3) Involvment of Auditor at the time of SYS. Development to develop Audit Modules.
Stable APP. SYS. 4) Need Stable SYS. or Application for concurrent Audit
Miss Audit Trail 5) Missing Audit Trail: More likely to be used where Audit trail is less visible

MTP M.14(2) Need for Audit of IS ⇒ [CIMA'S IDEA] Impact of IS Audit on organisation

1) Computer - controlled use 2) IS Audit 3) Maintenance of privacy 4) Asset safeguarding standard 5) Incorrect decision making 6) Data loss 7) Computer Error 8) Computer Abuse 9) Data integrity objectives 10) System efficiency object 11) Sys. effectiveness obj. 12) Value of H/S & personnel

6.14 MTP M.14 * [DAR] **Major ways by which Audit Trails can be used to support security objectives. or Objective of Audit Trail**

⇒ 1) Detecting unauthorised Access

2) Reconstructing Events: Audit Analysis can be used to reconstruct the steps that led to event such as sys. failure, security violations, or application processing errors.

3) Personal Accountability: Audit trail can be used to monitor user activity at the lowest level of detail.

6.15 * **Two Main categories of Data Management Control**

1) Access control: Controls are established in the following manner: 1) User Access control 2) Data Encryption: keeping data in dbase in encrypted form

MTP M.15 ⇒ 2) Back-up control

↳ Various Backup strategies are given as follows:

DDLG

i) Dual Recording of Data → Two complete copy of dbase are maintained
ii) Periodic dumping of Data → Periodic dump of all or part of dbase
iii) Logging input Transactions → which cause changes to the dbase
iv) Logging changes to the data → copying a record each time it is changed by an update action

6.18 * **Major Processing controls.**

1) Run-To-Run Totals → These help in verifying data that is subject to process through diff. stages.
2) Reasonableness Verification → Two or more fields can be compared and cross verified to ensure their correctness.
3) Edit checks ↳ similar to data validation control
4) Field Initialization ↳ Data overflow can occurs
5) Exception Reports ↳ Report are generated to identify error in data processed

6.19 * **Major Audit issues of operational layer with reference to application security Audit.**

⇒ [UPS]

1) User Accounts and Access Rights
2) Password controls: In general password strength, length, age, non-repetition & automated lockout after 3 attempts
3) Segregation of Duties: As frauds due to lack of segregation increase across the world, importance of the segregation of duties also increases.

modual 6.33 * **Role of IS Auditor with respect to Physical Access control. (PAC)**

⇒ Auditor Review the Physical Access Risk & control to form an opinion on the effectiveness of Physical Access control. This involves the following.

[RCR]

1) Risk Assessment → risk assessment procedure adequately covers periodic & timely assessment of all assets.
2) Control Assessment: whether PAC are in place and whether they are adequately protect the assets
3) Review of Documents: examination of relevant documentation such as the security policies, procedure, premises plans, Building plan, Inventory plan

module 6.36 MTP N.14(2) * **Major Tasks performed by operating system**

➡ [3MMS Handling]

1) Scheduling Jobs 2) Managing Hardware & software Resources 3) Maintaining system security 4) Enabling Multiple user Resource sharing 5) Handling Interrupts: is a Technique used by OS to temporarily suspend the processing of one program to another prog.

... Records

Page No.
Date: / /201

8.8 * Cloud computing Models [IPS Network communication]

⇒ 1) Infrastructure as a service (IaaS)

MTP N.14(a) → 2) Platform as a service (PaaS)

3) Software as a service (SaaS)

4) Network as a service (NaaS)

5) Communication as a service (CaaS)

8.8 MTP M.15 * Characteristics of cloud computing [SAM PV HUM]

⇒ 1) 1) High scalability: Enable servicing of Business requirement for larger audiences through high scalability.

2) 2) Agility: cloud works in the "distributed mode" environment. It share resources among users and tasks, while improving efficiency & agility.

6) 3) High Availability & Reliability: Availability of servers is supposed to be high & more reliable. Chances of Failure are minimal

3) 4) Multi-sharing: Multi users & applications can work more efficiently with cost reductions by sharing common infrastructure.

7) 5) Services in Pay-Per-Use mode:

5) 6) Virtulization: This technology allows servers & storage devices to increasingly share & utilize applications by easy migration.

4) 8) 7) Performance: High level of performance

8) Maintenance: Cloud computing application are easier, because they are not to be installed on each user's com. & can be access from diff. place

8.9 MTP N.14(c) * Advantages of cloud computing → [CA BAS EASY, QUICK]

⇒ 1) Cost efficiency 2) Almost unlimited storage

3) Backup & Recovery 4) Automatic Software Integration

5) Easy Access To Information 6) Quick Deployment [illegible] once opt for this method of function

8.10 RTP N.14 * Challenges to cloud computing in Brief [CIA GTPL

⇒ 1) Confidentiality (→ Prevention of unauthorized disclosure) 2) Integrity (→ Prevention of unauthorized modification) 3) Availability

3) Governance 4) Trust 5) Legal Issue & compliance

6) Privacy 7) Audit 8) Data Stealing (चोरी) 9) Architecture

10) Identity Management and Access control

11) Incident Response 12) Software isolation 13) Application security

2020 8.9 * Emerging BYOD Threats: [DIAN]

1) Device Risks: It is normally in the form of "Loss of Device". Lost or stolen device can result in easy access to sensitive corporate information

2) Implementation Risks: It is normally in the form of "weak BYOD policy"

3) Application Risks: It is normally in the form of "Application viruses & Malware"

4) Network Risks: It is normally in the form of "Lack of device visibility"

It Refers to the Technology that allows Transmission of data via a computer without being connected to Fixed Physical Link.
- This is the fundamental principle of mobile computing.
- Mobile data communication has become a very important & Rapidly evolving Technology as it allows users to Transmit data, from Remote locations to other remote or Fixed locations through cellular networks.

4.09 * **Data & System Back-UP Techniques** (N.14)

[FD IM] 1) Full Back-UP 2) Differential BackUP: Last Full BackUP
3) Incremental BackUP: In this BackUP, Those File are backed UP which have changed since last Back UP.
4) Mirror BackUP: Identical to a full backup

DM:250 * **TYPES of Disaster Recovery Plan**

[EBRT] 1) Emergency Plan 2) BackUP Plan
3) Recovery Plan 4) Test Plan

OM-255 * **Alternative processing Facility Arrangement**

1) Cold site: • Maintain critical Resource & equipment in duplicate form at some off-site location • Low cost - Maintaining • Not provide loor. downtime elimination
2) Warm site: • Bet^n cold & Hot side • It is Better then cold & worse then Hot!
3) Hot site: • Simple technique • All most all the equipment & Resources of working data Center are maintain • Expensive • provid NIL Downtime
4) Reciprocal Agreement: Two or more organization agree to provide BackUP Facility to each other • Maintain Extra capacity to serve other party.

Rev-8.4 RTPEMTP N.14 **Goals of cloud computing [E-SCRAP] (N.14)**

⇒ 1) To Create a Highly efficient IT Ecosystem, where resources are pooled together and cost are aligned with the resources actually used.
2) To Scale the IT Ecosystem quickly, easily and cost-effectively based on the evolving Business Needs.
3) To Consolidate IT Infrastructure into more Integrated and Manageable environment.
4) To Reduce Cost related to IT energy Consumption
5) To Access Service and data From Any where & At Any Time.
6) To enable Rapidly provision of Resources as Needed
7) To Improve 'Anywhere Access' for ever increasing users

8.11 * **Mobile computing Benefits:**

1) It provide Mobile workforce with Remote Access to work order details, Such as work order location, contact info., completion date, asset History, Relevant warranties
2) It provides Remote Access to corporate knowledge at the Job location
3) It enables mobile Sales personnel to update work order status in real-time, Facilitating excellent communication.
4) It enables us to improve management effectiveness by quality, info. flow, & ability to control a mobile workforce at any time, from anywhere

7.4 * Objectives of IT

1) To Grant legal recognition for transactions carried out by means of electronic data Interchange (EDI) and E-commerce in place of paper based Methods of communication.
2) To Give legal recognition to Digital Signature for authentication of any information or matter.
3) To give legal recognition for keeping of Books of A/C by bankers in electronic form
4) To Facilitate e-filing of documents with Govt. Depart.
5) To Facilitate electronic Storage of data.
6) To Facilitate and give legal Sanction to EFT both Banks and Financial Institutions.
7) To amend the IPC, the Indian Evidence Act-1872, Banker's Book Evidence Act-1981, RBI Act-1934

6 * Impact of IS Audit on organization

Need ~~For~~ Or Audit of IS [CIMA's IDEA DSSV]

⇒ 6 1) Costs of Data loss: Data is a critical resource of an organisation For its present and Future Process and its ability to adapt and survive in changing environment.

2) Incorrect Decision Making: Managers are involved in detection, investigation and correction Processes. These High level decisions require accurate data to make quality decision Rules.

3) Maintenance of Privacy: Today, may confidential data are collected in a Business process and there is a fear ~~taset~~ of misusing this data Because privacy has eroded beyond acceptable levels.

4) Asset Safeguarding objectives: The Info. Sys. assets (HIS & data) must be protected by a system of Internal Control from Unauthorised access.

5) IS Audit: It is the process of attesting objectives that focus on Asset safeguarding & data integrity and Management objectives that include effectiveness & efficiency

6) Controlled evolution of computer use: Use of Technology and reliability of complex computer system cannot be guaranteed and consequences of using unreliable system can be destructive.

7) Cost of computer Errors: In a computerised enterprise environment where many critical business process are performed, a data error during entry or process would cause great damage.

8) Cost of computer Abuse: Unauthorised access to computer, Malwares, Unauthorised physical access to computer facilities and Unauthorised copies of sensitive data can lead to destruction of Assets.

9) Data Integrity objectives: It is a Fundamental attribute of IS Auditing. The importance of to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective of the decision maker, competition & market environment.

10) System Effectiveness objectives: Effectiveness of a system is evaluated by Auditing the objective of the system to meet business and user requirement.

11) System Efficiency objectives: To optimize the use of various information system resources along with the impact on its computing environment.

12) Value of computer Hardware Software & personnel: These are critical resources of an organization, which has a credible impact on its infrastructure and business competitiveness.

xRoot 6.21 * What are the controls that can be used to prevent system exposure against Internet & Intranet? [FCCER]

⇒ 1) Firewall 2) Controlling Denial of Service Attacks
3) Encryption
4) Recording of Transaction Log
5) Call back Devices: The call back devices requires the use to enter password and if authorized then call back device establish a connection.

xRoot 6.20 * What things auditor should consider while evaluating Internet & Intranet?

⇒ 1) Component Failure ⇒ Failure of communication lines, Hardware, Software
2) Subversive Threats ⇒ intruder attempts to violate the integrity of some components in the sub-system by...
2 Intruders i) Invasive Tap: By installing it on communication line & either read or modify data.
ii) Inductive Tap: it monitors electromagnetic transmission & allows the data to read only.

xRoot 6.18 * System Development controls: [UTI UPS]

⇒ ~~1) System Authorisation Activities~~
1) User Specification Activities: Users must be actively involved in the sys. development
2) Technical Design Activities: The Tech. Design Activities in SDLC translate the user specification requirement into Tech. Spec.
3) Internal Auditor's Participation: Internal Auditor plays an important Role
4) User Test & Acceptance Procedures: Just before implementation, the individual modules must be tested.
5) Program Testing: All program modules must be thoroughly tested before they are implemented
6) System Authorisation Activities: All system must be properly Authorised.

xRoot 6.16 * How should conduct application security Audit?

xRoot 6.27 * Discuss Major Audit issue of Tactical Layer with Reference to Application Security Audit. [UP A I IT]

⇒ 1) User Profile: Auditor should check that any updates to user profile, like creating/deleting & changing of User Account
2) IT Risk Management: Assess Risk, conduct Regular Security awareness program, monitor peripheral security
3) Interface Security: It means interface of one application with another application in an organization. Auditor need to understand flow of data
4) Audit logging & Monitoring: Regular monitoring the Audit logs is required. However, the same is not possible for all Transaction, so must be done on an exceptional Reporting basis

(UPS) * Audit Issue of Operational Layer with Ref. to APP. Sys. Audit: (UPS)
1) User Account & Access Right 2) password controls 3) Segregation of duties

6.8 * Explain the set of skills that is generally expected of IS Auditor.

=) KUP:

Knowledge: ① Business (Sound operation, practice), ② IT strategies (Policy, Procedural control), ③ Professional Standard (Good)

Understanding: ① Info. Risk & controls, ② Tech. & Manual control

Professional Qualification & Certificates.

* Audit Hooks: • These are Audit Routines • that Flag suspicious Transactions.

* SCARF: • The SCRAF Technique involves • embedding audit software modules • within a host app. system • to provide continuous monitoring of the sys. trans.
• The Info. collected is written on Special Audit File the SCARF Master File
• In ~~Many~~ Many ways, the SCARF technique is like the Snapshot technique

* Audit Trail:
• Are logs that can be designed to record activity at the system, application, and user level.
• Maintain a chronological record of all events that have occured in a system.
• Provide an important detective control to help accomplish security policy objectives.

* Snapshots or extended Records:
• Tracing a Transaction in a computerized sys. can be performed with the help of Snapshots or extended Records.
• The snapshot software is built into the sys. at those point where material processing occurs which takes images of the flow of any transaction as it moves through the application.
• These images can be utilized to assess the authenticity, accuracy and completness of the processing carried out on the transaction

Page No.
Date: / /201

4.6 * Objectives & Goals of BCP: Primary objective of BCP is to enable an organization to survive a disaster & Re-establish normal business operation

=> Objectives:

1) Provide for the safety of people on the premises at the time of disaster.
2) Continue critical Business operation
3) Identify critical lines of Business & Supporting Function
4) Minimise the duration of serious disruption to operation and resources.
5) Minimize ~~tos~~ immediate damage & losses
6) Establish Mangt. succession & emergency powers
7) Facilitate effective co-operation of Recovery tasks.
8) Reduce the complexity of Recovery effort.

Goals:

1) Identify weakness and implement a disaster prevention program
2) Minimize duration
3) Facilitate effective co-op. of Recovery tasks.
4) Reduce complexity of Recovery effort.

4.7 * Phases of Methodology of developing a BCP? What is major point on which Methodology mainly emphasizes upon?

=> The Methodology emphasises on the following:

1) Providing Mangt. with complete Understanding of Total Efforts required to develop and maintain an effective Recovery plan.
2) Obtaining commitment from appropriate management to support and participate in the effort.
3) Defining Recovery Requirements from the perspective of Business Analysis
4) Document the possible losses, Recovery Task & Procedures.
5) Focusing on disaster prevention & Impact Minimisation as well as orderly & timely Recovery from Disaster.
6) Developing BCP that is understandable, easy to use & Maintain
7) Selecting proper Business continuity planning Teams.
8) Integrate the BCP into on-going other Business planning processes.

Page No.
Date : / /201

* Eight Phases of BCP (PVIRD TIM)

1) Pre Planning Activities
2) Vulnerability Assessment and General Destination of Requirements
3) Business Impact Analysis
4) Detailed Derivation of Requirements.
5) Plan Development
6) Testing Program
7) Maintenance program
8) Initial Plan Testing & Plan ~~Mai~~ Implementation

* Stage of SDLC (IRDATIM)

1) Preliminary Investigation
2) Requirement Analysis or Sys. Analysis
3) Design of system.
4) Acquisition & development of Software
5) System Testing
6) Implementation & maintenance.

2.1

1) Principal components of a TPS? [IPSO]
2) Features of TPS [LABS]
3) characteristics of an effective MIS. [CMISCMLC]

[NNN BP High] 4) Constraints in operating a computer Based MIS. [DELHI]
5) Example of DSS in A/cting or Accounting Application of DSS.
6) Components of DSS? [UPMD]
7) Components of ES? [IN U.K.K. Explanation Facility]

[LOW LEVEL & LACK OF FDI] 8) Briefly Describe Five Major characteristics of the Types of Information used in Executive Decision Making.
9) Pre-Requisites of MIS?
10) Attributes of Information? [TRMR 2011 CA CPT Q] VF

P.S.36 11) Limitation of MIS => Quality, Quantitative, flexibility, Effectiveness } • Adhoc - Tailor made } • Subsitute - Semism & customized
12) characteristics of DSS

RTPM.15 13) Discuss Diff. Types of Info. System => Diff. info sys. that serve diff organizational level. i) operational Level sys. 2) knowledge level sys 3) management level 4) strategic level sys.

MTP.M.15 14) Discuss I.T & its components? what are the activities carried out by IS in general

1.0.12 1) key Magt. practices, which are required for aligning IT strategy with enterprise strategy [UADCDC]
2) Risk Magt. Strategies. [5T]
3) Principle of COBIT-5 [MCA E Se]

[CAMADR] 4) Key Magt. practices for Implementing Risk Management
5) Areas which should be Reviewed by internal Auditors as a Part of the ~~review of~~ review of Governance, Risk and compliance (GRC)

[MR PIPESE] 6) key Magt. Practices for assessing and evaluating the system of Internal control in enterprise in details.

MTP N.14 7) What are the key Governance practices of GEIT? [EDM] → Governance system

MTP N.14 8) what do you understand by the Terms of COBIT? Describe its Practices in Brief? [IOC Obtain]

(WB)

RTP MTP N.14(2) 1.18 RTPM.15 9) Key Governance practices of Risk Management → Evaluating RM => Evaluate Risk magt. Direct risk magt. Monitor risk magt.

RTPM.15 10) COBIT & its components (1) framework (2) process discriptions (3) control objectives (4) magt. guide lines (5) maturity models.

P.S.30 RTPM.15 11) Benefit of Governance

Ch:3 MTPN.15(2)

1) Type of Info. Sec. Policy & Their Hierarchy. [USA ON CC]

4 MTPN.14 2) Five Interrelated components of Internal Control [IC RCM]

MTPN.14(2) 3) Major Financial control Techniques [ABCD IS OSS]

MTPM.15 4) Major Boundary Control Techniques [CBI PP]

5) Explain different classifications of Information

N.14 MTPM15(2) 6) Major Data Integrity Policies. [VS DDOQ]

7) Explain Various forms of Asynchronous Attacks
1) Data Leakage 2) Wire-Tapping 3) Piggybacking 4) Shutdown computer/Dele of ser

Computer Crime Exposure MTPN.14 8) Major Dimensions under which the impact of cyber fraud on enterprises can be viewed. [FLLDS]

MTPN.14 9) Major Techniques to commit cyber frauds

MTPN.14 10) Detective controls 10a) Preventive control

PN.14(2) 11) Impact of Technology on Internal control [PC RAM Se Authorization]

MTPM.15(2) 12) Key components of good security policy Effect of computer on

Ch:6 Effect of computer on Audit?

1) Issue Relating to Performance of evidence collection and Understanding the Reliability of controls [DAN LAL]

MTPN.14 MTPN.14(2) 2) Major Types of IS Audit [SISTEM] category of IS Audi

3) Major Stages (Steps) of IS Audit [SPF And Reporting Closure]

4) various Types of Information collected by using SCARF [A3S3P]

MTPN.14 5) Advantages of continous Audit Techniques

6) Disadvantages " " "

PN.14 7) Major ways by which Audit Trails can be used to Support Security objectives or [DAR] Objective of Audit Trail MTP:N14

8) Two Main Catagories of Data Management control [A B]

9) Major processing controls. [Run

10) Major Audit issues of Operational layer with reference to application Security Audit [UPS]

11) Role of Is Auditor with respect to Physical Access control [RC

MTPN.14(2) 12) Major Tasks Performed by Operating System. [3 Mms Handling]

13) Need for Audit of IS? [CIMA's IDEA]

XRDX-620 14) Internet & Intranet control?

MTPN.14 15) Discuss various output control in details [PLS Retention Storage Report]

XRDX 6.25

8) Integrate the BCP into on-going other Business planning processes.

3.8
1) Types of IS Polices & Their Hierarchy [USA ON CC]
2) Five Interrelated components of Internal controls [ICRCM]

5.14
3) How the Analysis of present SYS. is made by the SYS-Analyst?
2) Two primary Method, which are used for Analysis of the scope of a project in SDLC.
3) What are Sys. Development Tools? Major Tools used
4) for SYS. Development [CID System Process]

RTP M.15
4) Major Reasons due to which organizations fail to achieve their system Development objectives.
5) Major characteristics of Good Coded Program [UAE RRM]

M.14 Case
6) Five categories of Tests that a programmer Typically Performs on a Program Unit (Types of Testing) [FPPSS]
7) Changeover Strategies used for conversion from old To New. [DPSP]
8) Various Activities that are involved for successful conversion with respect to a computerized infor. system. [PFSSA]
9) Feasibility Study.
10) Fact-finding Techniques. [Doc. Obser I Q]
11) Stages of SDLC [IRDATIM]

5.18
12) What r the possible Advantages of SDLC from the perspective of IS Audit?
13) Categorized the System Maintenance.

RTP M.15
14) Types of Sys. Testing & Discuss Sys. Testing

MTP. M.15(2)
15) What issues would you like to raise during the Tech. feasibility of new proposed system?
16) Method of validating vendor proposal → Check list, Public evaluation Report, Point scoring Analysis
17) Post Implementation Review
18) Sys. Maintenance

PAGE NO.
DATE

8 or 8 MTP N.14 (2) 1) Cloud Computing Models [IPS Network communication]
2) Characteristics of cloud computing [SAM PV HUM]
MTP N.14 (2) 3) Advantages of cloud computing [CA BAS EASY, QUICK]
RTP N.14 4) Challenge to cloud computing in Brief
5) Emerging BYOD Thests [DIAN]
CH: 4 6) Data & System Back-UP Techniques
MTP N.14 Oct 18 RTP N.14 6) Goals of cloud computing [E-SCRAP] →
MTP N.14 Nov 18 7) Mobile computing Benefits

CH.6 Effects of computer on Audit?
1) Issue Relating to performance of evidence collection and understanding the Relicability of control [DAN LAL]
MTP N.14 2) Major TYPES of IS Audits (or) Catagaries of IS Audit [SIS TEM]
3) Major stages (steps) of Is Audit. [SPF And Reporting Closure]
4) various TYPES of Info. collected By Using SCARF [A3S3P]
5) Major ways by which Audit Trails can be used to support Security objectives (OR) OBJectives of Audit Trail [DAR]
6) Major Tasks performed by operating system? (Cases of operating SYS control?) [3MMS Handling]
7) Two main Catagories of Data Management Control [A B]
• 8) System Development Control [UTI UPS]
• 9) what Things Auditor should consider while evaluating Internet & Intranet [CS]
• 10) what are the controls that be used to prevent system exposure against internet & Intranet? [FCCER] 1) Firewall 2) Controlling DOS 3) Encryption 4) Recording Transcring 5) Cert Digital Service
11) Major Processing Control [Run ...
N.14 • 12) various output contol in details [PLS Retention Storage Report]
13) Major Audit Issue of Operational Layer with reference to Application security Audit? [UPS]
• 14) Major Audit Issue of Tactical Layer with Reference to Application security Audit? [UPAIIT]
• 15) Impact of IS Audit on organization? [CIMA's IDEA DSSV]
Need for Audit of IS.
16) Role of IS Auditor with Respect to Physical Access Control. [RCR]

* ITIL: Contains Best Practice For Providing IT Related Services.
used by Service organization → Bank, Telecom org., Software co.
5 Books: 1) Service Strategy 4) Service Operation
2) Service Design 5) Service Improvement
3) Service Transition: This Provide Best Practice For developing and implement designed service.

CH: 8

Note: 2 P.9. 45 ISO-27001 or ISMS Provides the following Four Phase for establishing I.S. Security:

Select control → 1) Plan Phase: This phase provides Procedure and standered for Planning I.S. Security
Implement control → 2) DO Phase → primarily Provide Procedure for implementing selected control
Evaluate control → 3) Check Phase → Procedure for evaluating the effectiveness of implemented control
Correct control Improvement → 4) Act Phase → Provide procedure for improvement & corrective actions for implemented controls.

Book: 2 P.96 * Principle of COBIT-5 [MCAUS]

1) Meeting Stakeholder Need
2) Covering EnterPrice End-To-End
3) Apply Single Integrated Framework
4) Use a Holistic Approach
5) Separate Governance from Management

* Benefit of COBIT-5 [MAAM OS]

High Quality info 1) Maintain High Quality info. To Support Business decisions.
Strategic goal 2) Achive Strategic Goals & Realize Business Benefit
Operations Excellence 3) Achive Operational excellence Through Reliable, efficient Application of Tech.
IT-Related Risk 4) Maintain IT-Related Risk at An Acceptable level.
Optimize cost 5) Optimize the cost of IT Service and Technology.
Compliance 6) Support compliance with Relevent Laws, Regulation Contractual Agreement & Policies.

* Enablers of COBIT-5.

Using All Interacting Components for establishing IT System:

1) Policies.
2) organizational Structure
3) Culture
4) Information
5) Infrastructure: Service / Application / Technology
6) Processes
7) People Skills and competances.