ISCA NOTES

PREFACE

These Notes have been prepared with the objective of Learning Headings of various points in an Answer.

For Example, IN CHAPTER-8, Emerging Technologies, there is a topic:

Pertinent issues in Cloud Computing

(1) Interoperability issues (2) Hidden costs.
(3) Unexpected Behaviours (4) Security issues
(5) Threshold policy.

→ A hint has been developed ~~to~~ to learn the above points in a Sequence.

These Notes cover only some of the Chapters and NOT the whole subject.

Also Latest Amendments for ~~NOVEMEB~~ NOVEMBER 2015 Attempt have NOT been covered in these Notes.

I can be reached at:
GARG7966@GMAIL.COM

PRATEEK GARG

INDEX

CHAPTER-8

EMERGING TECHNOLOGIES

(1) Cloud computing

(Last part)

In cloud computing:

(i) The consumer or user no longer has to be at a PC, i.e., user can use any device for using Applications.

(ii) The consumer does not purchase a specific version of software which is required to be configured for smartphones, PDA's and other Devices, i.e., can download the required version from cloud.

(iii) The consumer or end user does not own the infrastructure, software or platform in the cloud, this leads to lower upfront costs or capital expenses.

(iv) The consumer or user does not care about how servers and networks are maintained in the cloud

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

* Hint to Learn:

Cloud computing के क्या Benefits होते हैं?

(1) न तो Consumer/user को किसी 1 Particular Device की ज़रूरत ज़रूरत है (कोई भी Device use कर लो for using applications)

(2) न तो Consumer/user को किसी Device के लिए Specific version of software Purchase करने की ज़रूरत है (सीधा Cloud से Download कर लो)

(3) न तो consumer/user को Infrastructure, software or platform in cloud, को own करने की ज़रूरत है (i.e., Lower capital Expenditure)

(4) न तो Consumer/user को ये चिंता करने की ज़रूरत है कि Servers and Networks कैसे Maintained हैं Cloud में

(5) और Multiple servers को कहीं से भी Access किया जा सकता है by user, without Knowing where they are Located.

(2) Cloud computing Vs. GRID computing

(Do this topic from book → No Hint)

(3) PERTINENT ISSUES IN CLOUD COMPUTING

(i) Inter-operability issues
(ii) Hidden costs
(iii) Unexpected behaviours
(iv) Security issues
(v) Threshold policy.

* Hint to Learn:

Cloud computing में क्या दिक्कतें आती हैं ?

(i) User — एक ~~user~~ Cloud computing vendor से दूसरे ~~cloud~~ Cloud computing vendor में switch easily नहीं कर पाता (Inter-operability issues)

(ii) ऊपर से Cloud computing service providers Hidden costs नहीं न बताते users को

(iii) Consumers को Unexpected Results मिलते हैं cloud services से (Unexpected Behaviour)

(iv) अब जब इतनी सारी दिक्कतें हैं, तो हम कैसे मान लें कि हमारे Data को Extra Risk नहीं होगा (4) Security issues नहीं होंगी

(v) और हाँ, Cloud computing service providers को ध्यान रखना होगा कि जिस Period में उनकी Applications Excess में use होंगी, उस period को Handle करने के लिए अभी ही threshold policy बनानी है

(4) Software Development in Cloud

(Do this topic from Book → No Hint)

(5) Goals of cloud computing

(i) To create a highly efficient IT system where resources are pooled together.

(ii) Access services from anywhere at anytime.

(iii) Improve Anywhere Access for ever increasing users.

(iv) Reduce costs related ~~to~~ to IT energy / power consumption.

(v) Costs are aligned to what actual Resources are used, ie; pay only for what actually is used.

(vi) ~~Scale to IT system~~

(vi) Scale to IT system quickly, easily and cost effectively based on business needs.

* Hint to Learn: → Cloud Computing के Goals हैं:

(i) सबसे पहले एक Highly efficient system बनाना है

(ii) इस Highly Efficient system को ऐसे बनाना है कि services can be accessed from anywhere at anytime.

(iii) अब इस Highly Efficient System से users increase होंगे → So, for these ever-increasing users, Improve anywhere Access.

(iv) अब users को एक Benefit और मिलेगा, which is → costs related ~~to~~ to IT energy / Power consumption will get reduced.

(v) Service providers को users को एक और facility देनी है → ~~pay only~~ pay only for what actually is used.

(v) अब क्योंकि users को एक Highly Efficient system मिल रहा है → which can be accessed from anywhere → और जिस system से costs reduce हो रही है → तो अब इन सब Benefits की वजह से users will be able to scale to IT system quickly, easily and cost-effectively.

5

6 Cloud computing Architecture

(Do this topic from Book → No Hint)

7 Cloud computing Environment or Deployment Models (Types of cloud)

(Do this topic from Book → No Hint)

8 Cloud computing service Models

(Do this topic from Book → No Hint)

(9) Characteristics of cloud computing

(i) Maintenance
(ii) Performance
(iii) Agility
(iv) Pay per use Mode
(v) High scalability
(vi) Multi-sharing
(vii) High Availability and Reliability
(viii) Virtualisation

* Hint to Learn :

Cloud computing ~~soft~~ की कुछ ~~characteristics~~ Characteristics होती हैं, जैसे कि :

(i) क्योंकि Cloud computing software को Maintain करना Easy है

तो इसकी वजह से

(ii) Its Performance is high (+) (iii) Its Agility (Responsiveness for services) is high

इसके साथ-साथ Cloud computing से consumer को 2 benefits मिलते हैं :

(iv) Pay per use Mode
(+)
(v) High scalability (छोटे से छोटा या बड़े से बड़ा Business हो → किसी भी Level of Business Requirement को Cloud Computing Meet कर सकती है)

अब इन सारे Characteristics की वजह से ज़्यादा से ज़्यादा Consumers Attract होंगे Towards Cloud Computing

(vi) इसलिए ज़्यादा Consumers को एक साथ Handle करने के लिए, there is a facility of Multi-sharing.

(vii) अब जब इतने सारे Consumers आ जाएँगे, तब Cloud computing के Service Providers को users को High Availability and Reliability देनी होगी (i.e., Providing services on 24x7 basis with high Reliability) → so that Consumers services को use करना बंद न कर दें।

(viii) Virtualisation → No Hint.

PLEASE DO THE REST OF THE CHAPTER FROM BOOK

CHAPTER - 5

Acquisition, Development and Implementation of Information Systems

(1) Business Process Design
(2) System Development Process
(3) System Development Life cycle

→ Do these topics from Book
↓
No Hint

---

(4) Reasons of Failure to achieve System Development Objectives

(i) Lack of Senior Management support and Involvement
(ii) Difficult to define the Exact Requirements Particularly for Unstructured or Strategic system.
(iii) Changing User Needs.
(iv) Resistance to change
(v) Lack of users participation
(vi) Lack of Standard Project Management and system development methodologies
(vii) over-worked or under-Trained Development Staff
(viii) New technologies
(ix) Inadequate testing and User Training.

* Hint to Learn

जब हमने ये पता लगाने की कोशिश की कि System Development के objectives Achieve क्यों नहीं हो पा रहे, तो हमारे पास 2 storey सामने आई जिससे हमें पता चला कि Organisation में चल क्या रहा है.

↓
दो Storey ये हैं:
↓

(i) Users of system ने मिलकर ये Complaint की → कि there is a Lack of Senior Management Support and Involvement
↓
तो ये Complaint सुनकर Senior Management अपनी Support लेकर Users के पास आई
↓
फिर अब Users को कुछ Problems सामने आई, जैसे कि:

(ii) It is difficult for users to define the Exact requirements. Particularly for Unstructured or strategic system.

(iii) ऊपर से → Users की Needs from system, frequently Change होती रहती हैं (Changing user Needs)

(iv) और तो और New system Develop होने के बाद working Environment में जो Changes होंगे, वो Changes Changes Users को पसंद नहीं हैं, So, there is a resistance to Change.

(v) So, इन सब problems की वजह से users ने System Development में participate करना बंद कर दिया (Lack of users participation)

↓

फिर, जब System Developers ने System Development का काम start किया, तो उसमें कई problems आई, जैसे कि:

↓

(vi) ये पता चला that there is a Lack of ~~Stan~~ Standard Project Management and System development Methodologies. (अगर Standard Methodologies follow नहीं होती, तो It is diffi'alt to complete the system within Stipulated time and Budget)

(vii) ऊपर से Development staff over-worked or Under-trained है

(viii) और New technologies को Use करना भी Difficult हो गया है। (because of Lack of skilled Manpower Available and High Cost Involved)

(ix) और, Finally, जो New system बना, उसमें Testing + User training अगर Inadequate होगी, तो System तो fail होगा ही (Inadequate Testing and user training)

→ System Development Approaches

Following are some Approaches ~~for~~ or Methodologies for system Development:

→ Traditional or waterfall waterfall Approach.
→ Prototype Approach.
→ Incremental Approach.
→ Spiral Model.
→ Agile Methodology
→ Rapid Action Development Approach. (RAD)

(ii) Prototype Model

There are some Disadvantages of Prototype Approach.

(1) Prototype Model can be successful only if the System Developers are ready for providing significant ~~ty~~ time to experiment and build prototype and get it checked from Actual users again and again, until user Approves the prototype.

(2) Sometimes, to save Development time, developers do not ~~not~~ thoroughly test and Document the System because of the time consumed in experimenting with prototype, which may cause an inefficient and erroneous System Development

(3) Sometimes, Developers are unable to meet the Requirements in Actual system as shown in the prototype to users; which may cause ~~dissatisfy~~ dis-satisfaction in the system users during Actual use

* Hint to Learn

Prototype Approach की ३ Disadvantages हैं:

(1) सबसे पहले तो Prototype Model तभी Successful हो सकता है जब System Developers Significant time दें to experiment and build prototype और उस Prototype को Actual users से बार-बार Check करवाएँ, until user Approves the prototype (मतलब Time + मेहनत चाहिए → पर करें कौन)

↓

(2) अब Developers, Development time save करने के लिए क्या करते हैं → जो हमने 1st point में Discuss किया था कि Experimenting with prototype में Significant time चाहिए ✓ → उस Experimenting में तो Time लगा देते हैं → But Testing and Documenting of system को Time नहीं देते, which causes inefficient and erroneous system Development.

(3) अब Developers ने Prototype में जो भी ~~चीज़ें~~ Requirements बताई थीं, जब Actual system बना तो वो उन Requirements को Fulfil/Meet नहीं कर सका → which causes Dis-satisfaction in system During Actual use.

Next topic

→ Methodology of system Development] DO FROM BOOK
→ System Development Life cycle] ↓ No Hint.

→ Phase I of SDLC

Preliminary Investigation

(Do from Book → No Hint)

→ Phase II of SDLC

System Analysis or Requirement Analysis

The following Activities are performed in this phase:

(1) Collection of Information.
(2) Analysis of current system
(3) Analysis of proposed system
(4) Preparation of Management report or SRS Document.

→ (2) Analysis of current System

This Analysis covers the following Areas:

(i) History of the organisation
(ii) Inputs
(iii) Methods, Procedures and Data Communications.

(iv) outputs
(v) Data files maintained.
(vi) Internal controls.

* Hint to learn:

हमें current System Analysis में किन चीज़ों को Analyse करना है?

(i) सबसे पहले organisation की History को Analyse करो
(ii) फिर organisation के Inputs को Analyse करो
(iii) फिर organisation के methods, procedures and Data communications को Analyse करो
(iv) फिर outputs को Analyse करो

→ Hint for (ii) + (iii) + (iv) points
(Inputs → Procedures → outputs.)

(v) अब जो [Inputs → Procedures → Outputs] का Process है → इस process से कुछ Data files बनी होंगी → उन Data files को Analyse करो

(vi) और इस पूरे system को ठीक से चलाने के लिए कुछ Internal controls Apply किए होंगे organisation ने → उन Internal controls को Analyse करो

Next topic

→ System Development tools
→ Some Important System Development tools

Do from Book
↓
No Hint

→ Role of Different persons during SDLC Phases

Following are key persons/groups involved in a system development:

1. Steering Committee
2. Project Managers
3. Project Leader
4. Module Leader / Team Leader
5. Quality Assurance team
6. System Analyst / Business Analyst
7. Programmers / coders / developers
8. Data base Administrators.
9. Testers
10. Domain specialist
11. IS Auditor.

* Hint to learn

वो कौन लोग हैं, जो Project को Supervise करते हैं ?

① ~~Steer~~ Steering Committee
↓
② Project Manager
↓
Project Manager works with
③ Project Leader
④ Module Leader / Team Leader
⑤ Quality Assurance team.

Question: अब ये supervisor लोग किन लोगों को supervise करते हैं ?

ANSWER: ये उन लोगों को supervise करते हैं जो Actually System development का काम करते हैं, जैसे कि

⑥ System Analyst
⑦ Programmer / Coder / developer
⑧ Database Administrator
⑨ Tester.

⑩ अब ये पूरी Team अगर किस देश ↓ Project को Develop करती है, which is a New field for it, in terms of Applications Logics → Then, help of DOMAIN SPECIALIST is taken

⑪ और इस पूरी Team ने जिन Applications पर काम किया है, उन Applications की Development and Testing के दौरान Adequate controls ~~obs~~ observe किए गए हैं या नहीं
→ ये Ensure करेंगे Information System Auditor (IS Auditor)

Page 19

Page 20

Phase 3 of SDLC

System Design

→ A good system Design should have the following characteristics:
(Design principles)

(1) Design should be based on Extensive Analysis.
(2) It should follow laid down standards of Design
(3) It should be easy to understand
(4) It should be easily Adaptable to change, i.e., easily Maintainable
(5) Design should be Modular
(6) ~~It should be efficient Design.~~
(7)
(6) A good design should capture all the functionalities of system correctly.

(7) It should be efficient design
(8) Functions designed should be directly relevant to the business Activities.

* Hint to Learn

एक अच्छे System design के ये characteristics होते हैं:

(Design principles)

(1) एक Design जो Extensive Analysis पर Based होना है
(+)
(2) वो Design → standards of Design को भी Follow करता है
↓
ऐसा Design हमेशा

(3) Easy to understand होगा (+) (4) Easily Adaptable to Change होगा (i.e., Easily Maintainable)

(5) अब वही Design अगर Modular भी हो
(+)
(6) अगर ये Design सारी Functionalities of System को correctly capture कर सके
(7) तो ऐसा Design जिस में इतनी सारी Characteristics हैं
↓
(7) ऐसा Design हमेशा Efficient होगा

(8) और 1 बात को मत भूल जाना → कि System Design करते वक्त जो Functions Design किए हैं
→ Such functions should be directly Relevant to business Activities.

→ The system Design phase Mainly Consists of following Activities:

(1) Architectural Design
(2) Design of Data/Information flow
(3) Design of Database
(4) Design of user Interface
(5) Physical Design
(6) Design of Acquisition of hardware/system software.

* Hint to Learn

System Design Phase में कुल 6 Activities होती है, जैसे कि:

(1) सबसे पहले Architecture का Design तैयार करो
(2) फिर इस System के Architecture में Data कैसे Flow करेगा → इसका Design तैयार करो (Design of Data/Information flow)
(3) ये Data किसी न किसी Database में maintained होगा → तो उस Database का Design तैयार करो

(4) अब अगर User को Data का use करना है, तो User Interface चाहिए → इस User Interface का Design तैयार करो (which includes design of outputs and Inputs of a system)
(5) Then we create Physical Design.
(6) अब ये सारे काम करने के लिए Hardware (+) Software Acquire करने पड़ेंगे → तो Design of Acquisition of Hardware (+) Software तैयार करो

→ Architectural Design
→ Design of Data/Information flow
→ Design of Database

Do from Book
↓
No Hint

→ Design of user Interface

Output Design

The following factors are Normally considered while Designing output of a system:

(i) Content
(ii) Volume
(iii) Form
(iv) Timeliness
(v) Media
(vi) Format

* Hint to Learn

~~सबसे~~

output को design करते समय किन factors को ध्यान में रखा जाता है:

→ सबसे पहले, output के अंदर जो Data है

① वो Data किस Type का होना चाहिए (Content) (eg: customer Data, employee Data)

② वो Data कितना होना चाहिए, i.e, Amount of Data required in output (Volume)

→ अब जो output हमें मिल रहा है

③ वो output किस Form में present होना चाहिए To the user

④ वो output हमें कितनी Frequency में चाहिए (Timeliness)

⑤ वो output हमें किस medium के through चाहिए (Media)

⑥ वो output हमें किस Format में चाहिए (i.e, output Data कैसे Arranged होना चाहिए)

ONLY FOR UNDERSTANDING

Difference between Form and Format

Form	Format
→ It means the ways in which the content is presented to the user	→ It refers to the manner in which output data is arranged
→ eg: text, graphics, video, Audio, etc.	→ eg: Tabular and graphical format

AN EXAMPLE FOR UNDERSTANDING

For example, there is a detailed commercial information which has to be presented to the user. So, such an information → is presented in Text → and such text is arranged in Tabular format

Text = FORM
Tabular = FORMAT

→ Input Design
→ Physical Design
→ Design of Hardware and System Software platforms
→ Internal controls for Design phase

↓

Do from Book → No Hint

Phase - IV of SDLC

System Acquisition and Software Development

(Hint for only Advantages and Disadvantages of Application Packages is written here, Do the rest of the part of Phase IV from Book)

→ **Advantages and Disadvantages of Application Packages**

Advantages of Application Packages

1. Quality
2. Cost
3. Low Risk
4. Rapid Implementation

* **Hint to Learn**

हमें कुछ Advantages of Application Packages पता चले हैं, जैसे कि:

(1) सबसे पहले हमें ये पता चला कि Application Packages Quality wise better output देते हैं as compared to in-house Development of software (Quality)

(2) फिर हमें पता चला कि there is a lower Cost of Application Packages as compared to in-house developed software or software developed in-house (Cost)

(3) फिर हमें ये भी पता लगा कि इन Application Packages को use करने में Risk भी Low है (Low Risk)

(4) तो जब इतनी सब कुछ पता चल ही चुका है, तो चलो भाई, जल्दी से इन Application Packages को Implement कर दो (Rapid Implementation)

Drawbacks / Disadvantages of Application Packages

1. Lack of Flexibility
2. Low Quality Documentation
3. Continuity
4. Partly useful Application.

* **Hint to Learn**

इन Package softwares के कुछ Drawbacks भी हैं:

(1) न तो ये Packages organisation के हिसाब से Flexible हैं (Lack of flexibility)

(2) ऊपर से आता तो Proper Documentation नहीं है या तो Documents की Quality Low है (Low Quality Documents)

(3) अब अगर Software Vendors Reliable न हो तो Package software में Changes लाने में दिक्कतें आती है → Hence, Problem in continuity.

(4) अब अब इतनी सारी दिक्कतें है, तो है ये Package softwares हमारे लिए सिर्फ Partly useful है और है (Partly useful Application)
(Such Package software may not cover the entire requirements of the Organization)

Next topic

→ Software Development: Programming Techniques and Languages

Characteristics of Good coded Programs
Program Coding Standards
Programming Language
Choice of Programming Language
Program Debugging
Program Documentation
Program Maintenance

Do From Book ↓ No Hint.

Phase 5 of SDLC

System Testing

Levels of Test

(i) Unit test
(ii) Integration Test
(iii) System Test
(iv) Acceptance Test

→ Unit testing

There are five categories of Test that a programmer typically performs on a program unit:

1. Function Test
2. Performance Test
3. Stress Test
4. Structural Test
5. Parallel Test

* Hint to Learn:

(PTO)

* Hint to learn:

1 बच्चा है ~~इसकी~~ जिसको आज बहुत Stress हो रहा है → जब उससे stress का Reason पूछा, तो उसने बताया कि:

→ आज उसका School में Unit test है

↓

उस Test के बाद उसकी एक Function (1) में

(2) Performance भी है

इसलिए वो Stress (3) में है

↓

अब उसने एक Planning बनाई → पहले उसने अपनी ~~Performance~~ Performance का एक Structure (4) तैयार कर लिया

और वो Structure कहीं Fail न हो जाए, तो इसको ध्यान में रखते हुए उसने एक Parallel (5) Plan भी बना लिया

→ Integration Testing

(Do this topic from Book → No Hint)

→ System Testing

The System Testing may include the following Tests:

(i) ~~Stress or volume Testing~~
(ii) Performance Testing
(iii) Security Testing
(iv)

(i) Stress or volume Testing
(ii) Security Testing
(iii) Recovery Testing
(iv) Performance Testing

* Hint to learn:

मान लो कि → जो System है → वो एक CA student है जिसके Exams आने वाले हैं

(1) अब हमें ये check करना है कि क्या वो student (System) Stress को Handle कर पा रहा है

(2) अगर Handle नहीं कर पा रहा → तो उस student को और ज़्यादा Security दो (For example, by giving him proper food, nutrition, etc.)

(3) जब वो student अच्छे Nutrition लेगा, तब वो ~~थकावट (fatigue)~~ fatigue (थकावट) से Recovery अच्छे से कर पाएगा

(4) अब जब उसकी Recovery अच्छे से होगी और वो fresh feel करेगा, तो उसकी Performance Better हो जाएगी

→ Final Acceptance Testing
→ Internal control Aspects for system Testing Phase

Do from Book
↓
No Hint

PLEASE

PLEASE DO THE REST OF THE CHAPTER FROM BOOK

CHAPTER -3
PROTECTION OF INFORMATION SYSTEM

① Information System Protection and controls

(Do this topic from Book → No Hint)

② Need for Protection of Information System

→ Impact of Absence of Information system Protection on organisation

(i) Cost of computer Abuse / Misuse
(Like unauthorised Access to system, Malwares, viruses)

(ii) High cost of computer errors
(data error during entry or processing)

(iii) Cost of Data Loss.
(Data is critical Resource of an organisation, for its present and future prdress)

(iv) Cost of incorrect Decision Making.
(Management Decisions require Accurate Data. If there is an inaccurate Data, then there will be inaccurate/ incorrect Decision Making)

(v) Value of Hardware and Software and personnel (These are critical resources of an organisation)

~~(vi)~~

(vi) Reputation Loss due to Disclosure of Confidential Information.

* Hint to Learn:
ऐसे को नसे खतरे हैं जिनकी Cost organisation को bear करनी पड़ेगी in absence of information system protection:

(i) सबसे पहले तो Computer Abuse/Misuse का खतरा
↓
(जिसकी वजह से होगा
↓
(ii) Computer errors का खतरा
(+)
(iii) Data Loss का खतरा
↓
अब ① + ② + ③ points की वजह से, there are chances of:

(iv) Incorrect Decision Making

(v) अब इन सारे Points का Impact पड़ेगा on → Value of Hardware and Software and personnel

और इन सारे Points की वजह से सबसे बड़ा खतरा है :

(vi) Disclosure of Confidential Information
→ which may Result in Reputation Loss to the organisation.

→ If organisations apply Adequate protection or controls for their IT systems, they may achieve the following objectives:

Objectives of Information System protection and Controls

1. Improved Data Integrity
2. Improved Data security
3. Improved system performance
4. Improved system effectiveness (use)
5. Improved safeguard of Assets
6. Improved Reputation and customer Loyalty.

* Hint to Learn

Information system protection and controls की वजह से कौनसे Aspects Improve होने चाहिए ?

(1) + (2) points
→ Improved → Data
- (1) Integrity (Data protected Against unauthorised modification)
- (2) security

(3) + (4) points
→ Improved → System
- (3) Performance (Optimise use of IT resources eg: machine time, system software, Labour)
- (4) Effectiveness (whether system meets business and user Requirements)

(5) Improved → Safeguard of Assets

अब इन सारे Points की वजह से There must be :

(6) Improved Reputation and customer Loyalty.

Next topic

(3) Information system security

Objectives of Information security are:

		Abbreviation
(i)	Confidentiality	C
(ii)	Integrity	I
(iii)	Availability	A

* Hint to learn:

ये Security Agency है → C I A (Central Investigation Agency) → ये तीन objective है → Information की security.

(4) Why is Information Security Important?

(Do this topic from Book → No Hint)

(5) What kind of Information is Sensitive?

The following type of Information is normally considered as Sensitive Information:

		Abbreviation
(i)	Business operations Information	B
(ii)	Strategic plans	S
(iii)	Financial Information	F

* Hint to learn: Question

ये हमारी country की कौन सी एक organisation है जिसके पास Sensitive Information होती है

Answer → Border Security Force (B.S.F)

(6) Information security policy

(7) Tools to implement Information security policy: standards, guidelines and procedures

(Do these topics from Book → No Hint)

(8) Types of Information Security policies and their Hierarchy Relationship

Information security policy

(i) Organisation security policies
(ii) User security policies
(iii) Conditions of connection.

* Hint to learn Information security policies

(i) organisation की security policies

(ii) organisation के अंदर काम कर रहे users के

लिए Security policies.

(iii) बाहर से Users → Network को कैसे Access करेंगे (+) External Network से कैसे Connect होंगे → उसके लिए security policies (Conditions of connection)

→ Organisation Security policies

(i) Organisational Information security policy
(ii) Network and System Security policy
(iii) Information Classification policy.

* Hint to learn organisation Security policies

(i) organisation के अंदर

(i) organisation की Information के लिए Security policy

(ii) organisation के अंदर 2 होती है → Network and system → तो Network and system के लिए Security policy

(iii) अब Network and system के अंदर होती है Information → तो उस Information की classification (Classification के लिए Policy (Information Classification policy)

→ User security policies
→ Conditions of connection

Do from Book (P)
↓
No Hint

(9) Components of the security policy

A good security policy contains the following:

(1) Purpose and Scope of policy and its audience
(2) Security organisation structure.
(3) The Information System and its security Infrastructure, i.e, hardware and software
(4) Classification of Assets and their Inventory
(5) Access control Mechanisms
(6) Roles and Responsibility of following for Information Security:

→ Executives
→ Information system security professionals
→ Data owners
→ Processes owners
→ Technology providers
→ Users; and
→ IS Auditors

(7) Physical and Environment safety
(8) System Development and Maintenance Controls
(9) Network and Data communications Controls
(10) Monitoring and Audit Requirements
(11) Business Continuity planning
(12) Security Incident response and Reporting mechanisms
(13) Legal compliances.

* Hint to Learn:

एक Good security policy में क्या - क्या चीज़ें होनी चाहिए ?

(1) सबसे पहले ↓ Purpose and Scope of policy पता होना चाहिए

(2) फिर Policy में Security organisation structure Defined होना चाहिए

(3) फिर Information System और उसका security Infrastructure Defined होना चाहिए

↓

अब (2) + (3) points में जिस Structure/Infrastructure की बात की गई है, तो Structure किन चीज़ों से मिलकर बनता है → Assets + Assets में Access करने वाले users से

तो अब हमें ↓ Policy में बताना है कि :

(4) organisation के ↓ Assets कौनसे हैं और उनकी Classification कैसे की गई है

(5) इन Assets को Access करने के लिए किनसे कौनसे Access control Mechanisms लगाए हुए हैं

(6) जो लोग इन Assets को Access करेंगे → Like Executives, IS security professionals, Data owners, etc. → इन लोगों की Information Security के Regarding → ~~Roles~~ Roles and Responsibilities क्या है

(7) + (8) + (9) points

अब हमें organisation को 3 type के Security and controls provide करने हैं जिनके बारे Regarding policy में लिखा होना चाहिए :

(7) Physical and Environment security | (8) System Development and Maintenance Controls | (9) Network and data communication controls.

(10) Security provide करने के लिए ज़रूरी है कि हम जो काम कर रहे हैं → उसकी Monitoring and Audit भी हो → तो policy में Monitoring and Audit Requirements के बारे में लिखा होना चाहिए

(11) + (12) points

इतनी सब कुछ Defined होने के बाद भी अगर Business में कुछ गड़बड़ हो जाए, तो Business continued रखने के लिए 2 Aspects रखनी है:

(11) Business Continuity Planning

(12) Security Incident Response and Reporting Mechanisms.

(13) अगर ऊपर लिखे सारे Points पूरे होंगे, तबही तो Legal compliances को Fulfil कर पाओगे
→ Hence Legal compliances के Regarding बातें भी policy में लिखनी

→ Next topic
(10) Information System Controls
(11) Need of Controls in Information System

Do from Book
↓
No Hint

(12) Impact of Information Technology on Internal Controls

(The content in paragraph form is skipped here. Only hint for Learning headings of points is covered here).

→ Internal controls in a computerised Environment are implemented with goals of Information Asset protection, Data Integrity, System efficiency and Effectiveness.
This requires the following:

(1) Segregation of Duties
(2) Authorisation Procedures
(3) Record keeping
(4) Access to Assets and Records
(5) Management Supervision and Review
(6) Personnel
(7) Concentration of Programs and Data (Retention of Records on Data)

* Hint to Learn:

① ② ③ ④ ⑤ ⑥ ⑦
S A R A M P Concentration

Way of Learning the above abbreviation

Information Technology के आने की वजह से SARA (सारा) MP (Madhya Pradesh) के Internal Controls पर Impact पड़ा → ऐसा क्यों हुआ, इसकी वजह पर Concentrate करना पड़ेगा।

(OR)

Another way of Learning

Information Technology के आने की वजह से MP (Madhya Pradesh) के Internal Controls पर बहुत सारा (SARA) Impact पड़ा → ऐसा क्यों हुआ, इसकी वजह पर Concentrate करना पड़ेगा।

Internal Control components

A poorly controlled computer system is similar to a poorly controlled manual system. Internal controls for IT system comprises of the following Inter-related components

① Risk Assessment
② Control Activities
③ Information and communication
④ Monitoring
⑤ Control Environment

* Hint to Learn

अगर हमें Internal Controls को अच्छे से Implement करना है, तो हमें किन components पर ध्यान देना होगा:

① सबसे पहले हमें Risk Assessment करनी है
↓
फिर अगर Risk को Prevent करना है तो:
↓
② Control Activities को use करना होगा
↓
Control Activities को use करने के लिए:
↓
③ हमारे पास Appropriate Information होनी चाहिए, और Information को communicate भी करना है

(4) अब इन सारी Activities को Monitor करना भी ज़रूरी है

↓

(5) अब Management को एक अच्छा Control Environment create करना होगा, so that अब उपर वाले सारे Points अच्छे से ~~Implement~~ Implement हो सकें

(13) Information system Control techniques

(Do from Book)

Categories of control techniques

Functional Nature	IS Resources Controls	Objective of Controls
Known as General Control Framework	Known as IS Resources Controls	Known as Auditor categorisation of controls.

(14) Functional Nature of Controls or General Control Framework

This category divides controls into 3 categories

1. Accounting controls
2. Operational controls
3. Administrative controls.

(15) Objective of controls or Auditor categorisation of controls

The key objective of controls are prevention of Risks, detection and correction of Risks ~~or~~ Purpose of controls

These are also known as Auditor categorisation of Risks or Purpose of controls.

1. Preventive Controls
2. Detective Controls
3. Corrective Controls
4. Compensatory Controls.

→ Preventive Controls

These controls, as name suggests, are designed to prevent an error or any malicious Activity in the system, for example, using Login-id and Password is a preventive Control.

Broad Characteristics of Preventive Controls

Preventive controls are devised by:

1. Understanding probable threats (जिन्हें system के उपर हमला threats हैं)
2. Understanding vulnerabilities and Exposure of the

Assets for threats.
(हमें अपने Assets को Threats से बचाने में यहाँ कौन-कौन से Cvulnerability and Exposure)

(3) Finding the necessary preventive controls to avoid the probable threats.
(उन इन threats से बचने के लिए Preventive Controls को ढूँढेंगे)

Preventive Controls are implemented for both Computerised and Manual Environment, but techniques and Implementation may differ depending upon the types of threats and Exposure. Below list provides some examples of preventive controls:

(1) Employ qualified personnel
(2) Access Controls.
(3) Id- Passwords.
(4) Firewalls.
(5) Anti-virus software.
(6) Segregation of Duties
(7) Proper Documentation
(8) Authorisation of transactions
(9) Validation of transactions.

* Hint to Learn → Examples of Preventive controls

(1) Personnel → qualified होने चाहिए
(2) उन Personnel को काम दें System को Access करना → इसके लिए use Access controls
(3) Personnel जिस system को Access करेंगे → उस System में Id- Passwords use करो
(4) +(5) points
अपने System में Malicious Activities से बचने के लिए → Firewalls + Anti-virus software use करो
(6) अलग Personnel काम अलग से करें → उसके लिए Duties Segregated होनी चाहिए
(7) Personnel जो काम कर रहे हैं → उसकी Proper Documentation होनी चाहिए

(8) & (9) points
Personnel ने जो Transactions की हैं, वो Transactions Authorised + validated होनी चाहिए (Authorisation + validation of Transactions)

→ Detective Controls

As name suggests, these controls are used to detect errors or malicious Activities on system.

Broad Characteristics of Detective Controls

Detective controls are devised by:

(1) Having clear understanding of Unlawful Activities (जब unlawful unlawful activities को समझा होगा → तब ही उनको Detect कर पाएंगे)

(2) Controlling such Activities through preventive Controls. (जब unlawful Activities को control करने के लिए सबसे पहले preventive controls Apply करें)

(3) Establishing Detective controls which can report the unlawful Activities, if preventive Controls are not able to prevent such Activities. (जब preventive controls unlawful Activities को न रोक पाए, तो Detective Controls Establish करने होंगे जो unlawful Activities को Report कर सकें)

→ Following are some examples of Detective Controls:

(i) Frequent Audit
(ii) Audit trails controls
(iii) Revalidations of Transactions after Executions
(iv) Reconciliation of statements
(v) Monitoring Expenditure against Budgeted Amount.
(vi) Echo controls in Telecommunications.

[Hint: Validation of Transactions → Part of preventive controls
Revalidation of Transactions → Part of Detective controls]

→ Corrective Controls
→ Compensatory Controls

Do from Book → No Hint

(16) IS Resources control Techniques

(i) organisational controls
(ii) IS Management controls.
(iii) Financial controls
(iv) User controls
(v) SDLC controls
(vi) Data Integrity controls
(vii) Logical Access controls
(viii) Physical Access controls
(ix) Application controls
(x) Data Processing Environment controls

→ Organisational controls

The following are key organisational controls:

(1) Establishing organisation structure and Responsibility and Reporting structure.
(2) Clearly Defining Responsibilities and objectives of each function
(3) Defining Clear Job Descriptions.
(4) Segregation of Duties
(5) Establishing policies, standards, procedures and practices.

* Hint to learn:

Following are key organisational controls:

(1) सबसे पहले organisation structure (ए) Responsibility and Reporting structure को Establish करना होता है।
↓
(2) organisation structure बताता है Different functions से → तो हर Function के Responsibilities and objectives को Define करो
↓
(3) Functions को perform करने के लिए हमें चाहिए → Job Descriptions → So, Define Clear Job Descriptions.
↓
(4) अब अगर Jobs को सही से Perform करना है तो we should do Segregation of Duties.
↓
(5) और organisation के सारे काम ठीक से Perform हो सकें → उसके लिए ज़रूरी है → Establishing policies, standards, procedures and practices.

→ IS management controls

The following are key Management controls:

(1) Adopting an official IS organisation structure
(2) Responsibility
(3) An IT steering committee.

* Hint to Learn :

(1) एक Information System organisation structure adopt किया
↓
(2) Information system management को responsibility दी → of Information system controls
↓
(3) और एक IT steering committee बैठा दी

→ Financial controls

The following key controls are defined as financial controls:

(1) Use of source Documents in sequence
(2) Supervisor Review
(3) Authorisation
(4) Segregation of Duties
(5) Document each Task including Cancellation
(6) Safekeeping of Documents and Resources
(7) Establishing a Budget

* Hint to Learn

अगर किसी organisation में Financial controls लगाए जाएँ, तो उन controls के हिसाब से काम कैसे होगा ?
↓
(1) सबसे पहले Source Documents को Sequence में लगाया जाएगा
↓
(2) फिर source documents supervisor को दे दिये जाएँगे → for Review by Supervisor
(3) फिर supervisor source documents को Authorised user को देगा for Data Entry (Authorisation)
↓
(4) Authorised user अपना काम तब ही कर पाएगा जब Duties segregated होंगी
↓
(5) Authorised user अपने दिए Task को Document करेगा (Including Cancellation of Transaction) (Document each Task including cancellation)
↓
(6) फिर सारे Documents and Resources को Safe Location पर रख दिया जाएगा (Safekeeping of Documents and Resources)
(7) और इन सब कामों को करने के लिए एक Budget Establish करना भी हुत ज़रूरी है (and we have to verify these budgets with Actuals for any variations)

→ Data Processing Environment controls

(Do from Book)

→ User controls

- Boundary controls
- Input controls
- Processing controls

Do from Book
↓
No Hint

→ • Output controls

(a) Maintaining Log of output programs Execution to know the details of communicated output
(b) Spooling/queue Medication control
(c) Controls over Printing
(d) Report Distribution.

* Hint to Learn

① लॉग (Log) → (Maintaining Log)
② बहुत देर से system cafe में queue में खड़े हुए हैं
③ और Printing का wait कर रहे हैं
④ और अब किसी ने कहा कि भाई → Print होने के लिए Report दे दी है, उसको जल्दी Distribute कर दो (Report Distribution)

→ Database Controls
(Do from Book → No Hint)

→ Audit trail Controls

Objective of Audit trails

(i) Detecting unauthorised Access and Activities on system
(ii) Reconstruction of Events.
(iii) Personal Accountability

* Hint to Learn

Audit trail is used as Detective Control. जो हैकिंग पड़ चुकी है → उसको पता Audit trail से लगा सकते हो

Objective of Audit trails

Audit trail का objective है Detective का काम करना
↓
अब एक Detective के क्या काम होते हैं?

① अगर किसी ने unauthorised way में system को Access किया → तो इस Unauthorised Access को detect करो
(Detecting unauthorised Access and Activities on system)

(2) ऐसे सारे Events के जिनकी वजह से system failures हुए या Application errors हुई
→ उन Events को Reconstruct करो
(Reconstruction of Events)

(3) और सब users of Information System को इस बात से aware होना कि Audit trail control is being used to monitor/record these Activities → तो वो ऐसे ऐसे करेंगे and they will not conduct unauthorised Activities
↓
This is Establishing → personal Accountability

Next topic
→ System Development and Acquisition Phases Controls

(Do from Book → No Hint)

→ Controls over Data Integrity, privacy and security

• Information Classification
(Do from Book → No Hint)

(i) Top secret
(ii) Highly confidential
(iii) Proprietary
(iv) Internal use only

(v) Public Documents.

⇒ • Data Integrity

(Do from Book → No Hint)
There are 6 important Data Integrity controls:

(i) Source Data controls
(ii) Input validation controls
(iii) on-line Data Entry controls
(iv) Data processing and storage controls
(v) Output controls
(vi) Data communication controls.

⇒ • Data Integrity policies

Data Integrity policies include → Rules and procedures which help to maintain Data Integrity.
और ये जो Rules हैं → वो Ensure करते हैं
(1) Error free Data (2) Reconstruction of Data in case Data is destroyed.

The Key Data Integrity policies are:

(i) Updating Anti-virus system
(ii) Software Testing
(iii) Segregation of Duties or Division of Environment
(iv) off-site back-up storage
(v) Disaster Recovery.

* Hint to Learn:

जैसा कि अभी बताया कि Data Integrity policies ये Ensure करती हैं कि Data Error free रहे, तो अब ये कैसे Ensure होगा?

(1) सबसे पहले तो ये ↓ देखो कि Virus की वजह से Data में कोई गड़बड़ (Error) न हो
→ So, update Anti-virus system

(2) फिर देखो कि Software की वजह से Data-Processing में कुछ गड़बड़ न हो → So, Do Software Testing.

(3) फिर ये देखो कि Duties Mix-up होने की वजह से कोई गड़बड़ न हो → Hence, Do Segregation of Duties or Division of Environment.

(4) अब कुछ गड़बड़ होने से पहले हो Data का Back-up लेकर रख लो (Off-site back-up storage)

(5) इतना कुछ करने के बाद भी अगर कुछ Disaster हो जाए, तो Disaster Recovery के लिए Disaster Recovery plan होना चाहिए

→ Data security
(Do from Book → No Hint)

→ Access controls

Information system and its resources can have two types of Access:

(1) Logical Access
(2) Physical Access

• Logical Access controls

Logical Access controls are established with the following objectives:

(i) Allow Access of system to Authorised users only.
(ii) Restrict Access of Network to Authorised users only.
(iii) Restrict users to Authorised transactions only
(iv) Protect system from malicious programs and viruses, etc.
(v) Helps to protect the integrity of Application and Data, etc.

* Hint to Learn:

Logical Access controls के Objectives क्या हैं:

(i) Access of systems (I) — Allowed only to Authorised users
(ii) Access of Network

↓

System और Network को Access करने के लिए Authorised users हैं Transactions perform करेंगे

↓

(iii) Such transactions should be Authorised transactions.
(Restrict users to Authorised transactions only)

(iv) इसमें साथ-साथ अपने System को Malicious programs and viruses से भी सुरक्षित करना है

(v) ऊपर वाले सारे steps लेने से Applications और Data की Integrity protect होगी

Types of Logical Access Paths

(Do this topic from Book → No Hint)

Following are some common paths through which logical Access can be gained for an information system:

- Online terminal → Operator console.
- Dial-up ports.
- Telecommunication Link.

Possible Exposures/Revelations and Losses

We can divide the Exposures and Losses in the following 3 categories:

(i) Technical Exposures
(ii) Asynchronous Exposures/Attacks.
(iii) Losses or Impacts of Exposures.

→ Technical Exposures

This primarily includes Access through Malicious programs.

(a) Round down
(b) worms
(c) Trap doors
(d) Trojan Horse
(e) Logic Bomb.

(f) Salami Techniques
(g) Data Diddling.

* Hint to Learn

एक (a) Round (b) worm को (c) Trap किया और (d) House पर बैठा दिया और उस House पर (e) Bomb Fit कर दिया → ये सब करने के बाद उस House और worm को आखिरी सलामी (f) Salami दे दी गई → और हमको इस पूरे procedure process का (g) Data भी अपने पास रखना पड़ेगा।

इस पूरे काम को अगर हमको ठीक से करना है तो हमें Technical Exposure जानकर चाहिए

→ Asynchronous Exposure or Attack

This includes access of system through Network or Telecommunications link.

Some common Examples of this Exposure are:

(a) Hacking
(b) Piggybacking
(c) Eaves-Dropping
(d) Wire-Tapping
(e) Denial of service Attack

* Hint to Learn

Visualise this scenario

एक Terrorist organisation है जो एक Room में बैठकर Asynchronous Exposure or Attack की planning कर रही है और एक बन्दा (spy) उनकी बातें छिपकर सुन रहा है

(a) एक ~~Hacker~~ Hackee है → जो Room के बाहर खड़ा है

(b) वो एक Pig की Back पर चढ़ता है (Piggy backing)

(c) और उस Pig पर चढ़कर चढ़कर किसी तरह से उस Room की खिड़की तक पहुँच जाता है

(c) अब खिड़की तक पहुँच कर वो Hacker Eaves Dropping करने लगता है (छिपकर बातें सुनना)

(d) अब उसे पता चलता है, उस Room में कुछ लोग wire-Tapping कर रहे हैं

और

(e) Denial of service Attack की Planning कर रहे हैं

→ Losses or Impacts of Exposure

(a) Blackmail / Industrial Espionage
(b) Disclosure of confidential, sensitive or Embarrassing Information
(c) Legal issues
(d) Financial Loss
(e) Loss of credibility or Competitive Edge
(f) Sabotage

* Hint to Learn

~~Technical~~
Technical + Asynchronous Exposures की वजह से organisation को कौनसे Losses face करने पड़ेंगे:

Losses or Impacts of Exposures

एक Person है जो Regular Basis पर :

(a) एक organisation को Blackmail करता है
(b) और कहता है कि वो organisation की confidential Information को Disclose कर देगा।

अगर Information Disclose हो जाई तो :

(c) organisation Legal issues में फँस जाएगा

(+)

(d)(+)(e) इसके साथ-साथ organisation को Financial Loss (+) Loss of credibility face करना पड़ेगा।

(f) और अगर ये सब Actually हो गया तो organisation को Sabotage face ~~करेगा~~ करना पड़ेगा।

→ Logical Access violators
→ Types of Logical Access Controls
→ Access control Mechanisms
→ Physical Access Controls
→ Application Controls
→ BCP controls
→ Environmental controls
→ Cyber frauds

↓

[Do these topics from Book (No Hint)]

→ Controlling against viruses and ~~other~~ other destructive programs.

• Anti-virus Software.

following functions are performed by Anti-virus software:

(a) Scanning
(b) Integrity checking
(c) Virus Removing.

* Hint to Learn:

(a) सबसे पहले Program files, ~~or~~ memory, etc. को scan करके check किया कि virus है या नहीं (Scanning)

~~(b)~~

↓

(b) फिर अगर कोई unauthorised changes हुए हैं in any file, तो उनको detect किया (Integrity checking)

↓

(c) और Finally, virus code को virus infected files में से Remove कर दिया (virus removing)

CHAPTER - 6

AUDITING OF INFORMATION SYSTEM

(1) Controls and Audit

→ Need of controls and Audit for Information System

↓

Economic Losses and Impacts on organisation working due to absence of controls

- Cost of Incorrect Decision making
- Cost of Data Loss
- Loss of Hardware and Software values
- Reputation loss due to disclosure of confidential Information
- Loss due to computer errors
- Cost of computer Abuse/Misuse

→ Objective of controls and Audit of controls

- Improved Safeguard of Assets
- Improved Data security
- Improved System Effectiveness (Use)
- Improved System Performance
- Improved Data Integrity
- Improved Reputation and customer Loyalty.

* Hint for above mentioned topics has already been included in Notes of Chapter-3 (Protection of Information System) → (Pg 35 to 38 in these Notes)

→ Growing Importance, education and awareness about Information System controls and Audit

(DO from Book → No Hint)

(2) Effect of computers on Audit

(DO this topic from Book → No Hint)

The impact of computers in preparation and maintenance of financial books and reports can be summarised as follows:

1. Changes in Audit trail and Audit Evidence
2. Change in Internal Control Environment
3. New causes and sources of error
4. New Audit procedures and processes.

→ Change in type and Nature of Internal controls

(OR)

Change in Internal control Environment

(Hint for this topic has already been included in Notes of Chapter-3 (Protection of Information System)) → (Pg 46 in these Notes)

Next topic

Responsibility for Implementing Controls

→ Systematic steps taken by Information managers and IS Auditors for an effective control system are as follows:

(i) Develop and Implement appropriate cost effective Internal controls.

(ii) Assess the adequacy of Internal controls in programs and operations.

(iii) Seperately Assess the Adequacy of Internal controls over Information System consistent with security policy

(iv) Identify Needed Improvements

(v) Take corresponding corrective Actions

(vi) Report annually on Internal controls through Management Assurance ~~system~~ statement

* Hint to Learn:

Information Managers and IS Auditors किन Systematic steps को follow करते हैं, for an effective control system?

↓

(1) सबसे पहले तो Cost effective Internal controls Develop and Implement किए जाते हैं.

↓

अब ये check किया जाता है कि जो Internal controls develop हुए हैं, क्या वो Adequate हैं, तो इसके लिए हमें 2 चीज़ें Assess करनी हैं:

↓

(2) क्या Programs and operations में Internal Controls Adequate हैं

(+)

(3) क्या Security Policy के हिसाब से Internal Controls Adequate हैं

(4) अब अगर इस Assessment के बाद हमें पता चलता है कि Internal Controls Adequate नहीं हैं, तो फिर हमें देखना है कि कहाँ Improvement की ज़रूरत है (Identify Needed Improvements)

↓

(5) अब इन Improvements को Implement करने के लिए Corresponding corrective Actions लिए जाएंगे

(6) और Finally, इन सब चीज़ों की Reporting होगी, on an annual basis, through Management Assurance statement.

Next topic

(4) The IS Audit process

→ Responsibility of IS Auditor

A set of skills generally expected from IS Auditors include:

(1) Auditor should have requisite professional and Technical qualifications

(2) Auditor should have sound knowledge of business operations, practices and compliance Requirements.

(3) Auditor should have good understanding of information system risks and controls.

(4) Auditor should have ~~sound~~ knowledge of IT policies, particularly security policy.

(5) Auditor should possess good knowledge of standards and best practices of IT Controls and Security.

(6) Auditor should have ability to understand the technical controls.

* Hint to Learn:

IS Auditor के पास कौनसे skills होने चाहिए:
(Basically किन चीजों की knowledge + understanding होनी चाहिए)

(1) सबसे पहले तो IS Auditor के पास Requisite Professional and Technical qualifications होनी चाहिए

(2) पर सिर्फ qualifications से काम नहीं चलता → Auditor के पास knowledge + understanding भी होनी चाहिए

अब किन बातों की knowledge होनी चाहिए?

(2) सबसे पहले तो Business operations, practices and Compliance Requirements की knowledge होनी चाहिए

(3) और Information System को क्या Risks होते हैं और कौनसे Controls use होते हैं → इसकी good understanding होनी चाहिए

अब IS Auditor ने ये समझ लिया कि Information System को कौनसे Risks होते हैं, तो अब उन Risks को Materialise होने से कैसे Prevent किया जाता है, Auditor के ये समझ होना है

इसको समझने के लिए Auditor must have understanding of:

(PTO)

↓

(4) IT policies, particularly security policy
(+)
(5) Standards and best practices of IT controls and security
(+)
(6) Technical controls

→ Functions of IS Auditor

IS Auditors review the Risks related to IT systems, for example:

(1) Auditors review and check IT related frauds
(2) Auditors Review and check whether organisations have Adequate IT related policies
(3) Auditors check whether information security is Adequate
(4) Auditors review and check whether IT resources are efficiently utilised.
(5) Auditors Review and check whether System development and maintenance process is Controlled process or Not.

* Hint to learn :

Auditors Review and check
↓
IT related
① frauds
② Policies - Adequate or Not
③ Security - Adequate or Not.
④ Resources - efficiently utilised

(5) Auditors Review and check whether system Development and Maintenance process is Controlled process or Not.

→ Categories of IS Audits

IS audit is categorised in Five types, i.e., an IS Auditor audits the following broad Areas of Information System:

(1) Tele communications, Intranet and Internet.
(2) System Development
(3) System and Applications.
(4) Information processing facilities
(5) Management of IT and Enterprise Architectures

* Hint to Learn

IS Auditor को Information System की Audit करनी थी, तो इसके लिए उसने IS Audit को 5 types में categorise किया

↓

ये categorisation उसने कैसे की, हम इसका पता लगाते हैं:

↓

① सबसे पहले IS Auditor ने, Telecommunication, Intranet and Internet के through पता लगाया

↓

क्या पता लगाया?

↓

② यही कि System Development कैसे हुई है

↓

अब System Develop हो गया, तो उसने पता लगाया कि:

↓

③ System के अंदर Applications कौनसी हैं

↓

अब Applications का क्या काम है → उनका काम है Processing करना Information की

↓

④ अब Auditor ने check किया कि Information Processing facilities ठीक से काम कर रही हैं या नहीं

⑤ अब ये सारे काम ठीक से हों, उसके लिए Management of IT and Enterprise Architecture का ठीक (Adequate) होना ज़रूरी है

→ Steps in Information Technology Audit

Different organisations go for IS Audit in different ways; In general, IS Audit can have the following six steps:

① Scoping and Pre-Audit survey: Determine main focus Area for Audit

② Planning and Preparation: Planning the tasks in details for Audit to cover the focus area or the risks.

③ Audit work / Field work: Conducting Audit as per planning.

④ Analysis: This includes Analysis of Audit results.

⑤ Audit Reporting → Reporting Results to Management

⑥ Closure Notes: Closing Audit assignments with Required follow-ups.

* Hint to Learn:

In general, IS Audit can have the following six steps:

① WA WHAT TO Audit → Scoping and Pre Audit survey

(2) How To Audit → Planning and Preparation

(3) Conducting Tests / Audit / Reviews → Audit work / Fieldwork.

(4) अब Audit हो गई → उसके Results आ गए
→ अब इन Results का Analysis करो

(5) Audit Results को Management को Report करो
(Audit Reporting)

(6) अब Audit Assignment को Close करो with Required follow-ups (Closure Notes)

→ Audit के Standards and Best practices

(Do this topic from Book → No Hint).
Following are organisations and Associations providing best practices and Standards for IS Audit:

(i) ISACA (Information System Audit and Control Association)
(ii) Iso 27001
(iii) Internal Audit Standards
(iv) Standards on Internal Audit issued by ICAI
(v) ITIL (Information Technology Infrastructure Library).

Next topic

(5) Performing IS Audit

→ Audit planning → It is a Continuous process

In general, Audit planning includes the following key Activities:

(1) Obtaining understanding about Entity and its Operations.
(2) Obtaining understanding about Internal Controls mainly related to Information System.
(3) Assessing the various risks for Entity operation
(4) Designing the Audit procedures.
(5) Planning for timing and Extent of Audit procedures, etc.
(6) Identifying the significant issues in Audit process.

* Hint to Learn

Audit planning में कौनसी Activities include होती हैं?
↓
सबसे पहले तो Entity / organisation के Regarding इन 3 चीजों की understanding लेनी होती है:
↓
(1) इस Entity और उसके operations को समझना होता है
(2) Entity के अंदर जो Internal controls हैं (related to Information System) → उनको समझना होता है.

(3) Entity के operations को जो Risks हैं, उनको समझना होता है (i.e., Assessing the risks)

→ अब Audit procedures procedures से related - ये 3 Activities करनी होती हैं:

(4) Audit procedures को Design करना होता है

(5) Design हो गया, उसके बाद:
Timing and Extent of Audit procedures की procedures का plan करना होता है।

(6) और Audit process में Significant issues कौनसे हैं → उनको Identify करो

→ Methodologies of Audit of controls

(Do this topic from Book → No Hint)

CAFTER Methodologies of Audit of controls)

→ The following steps can be part of an effective IS Audit:

(i) Audit plan
(ii) Preliminary Review
(iii) Audit Evidence and Documentation.

→ Audit Plan
(Do from Book → No Hint)

→ Preliminary Review

The following are some of the critical factors, which should be considered by an IS Auditor as part of his/her preliminary Review:

(i) Obtaining knowledge about business.
(ii) Understanding the technology.
(iii) Risk Assessment and Materiality
(iv) Understanding the internal control systems.
(v) Legal considerations and Audit standards.

* Hint to Learn:

Preliminary Review करते हुए IS Auditor को इन critical factors का ध्यान रखना चाहिए:

(1) सबसे पहले Business की knowledge लो
(2) फिर Business को चला ने के लिए जो Technology use होती → उस Technology को समझो

(3) अब Technology use होगी, तो Technology की वजह से Risk भी होगा → तो Risk Assessment करो और Materiality को समझो

(4) अब Risks को control करने के लिए कौनसा factor use होगा → Internal Controls → तो Internal control systems की understanding लो

(5) Finally, Bussiness चलाने के लिए हमको Law की जानकारी होना बहुत जरूरी है → तो Legal Considerations and Audit standards को समझो

→ (Now, we are understanding points of preliminary review in detail):

(i) Obtaining Knowledge of Bussiness

It helps to conduct an effective Audit, if auditor is well-versed with entity's bussiness in terms of:

(a) Understanding general economic factors and industry conditions affecting the entity's bussiness
(b) Its products and services
(c) Understanding its clientele, vendors, strategic bussiness partners / Associates to whom critical processes have been outsourced
(d) Understanding level of competence of Top

Management and IT management.

(e) Finally, set-up and organisation of IT-Department are important factors to understand and it helps for conducting an effective Audit

* Hint to Learn

Auditor को Entity के Bussiness के किन Aspects की understanding लेनी होगी ?

↓

Auditor has to obtain knowledge (+) understanding of:

(1) Entity किस Environment में अपना Bussiness चला
(a) रही है, उस Environment के कौनसे Factors Entity को affect करेंगे → General Economic factors and Industry conditions → तो इन factors की understanding लो

(2) Entity कौनसे products and services provide कर रही
(b) है → इसको समझो

(3) अब Entity के products / services किनको provide कर रही
(c) है → clientele को
Entity के key products and services किनसे लेते रही है
→ vendor / suppliers से
Entity किनके साथ मिलकर काम कर रही है
→ Strategic Bussiness Partners / Associates से
(understanding its clientele, vendors, Strategic Bussiness Partners / Associates to whom critical processes have been outsourced)

(b) Entity को कौन लोग चला रहे हैं → Top Management
(d) + IT Management → तो इन लोगों की Level of competence की understanding लो

(e) और Entity को जो लोग चला रहे हैं → वो लोग Entity को operate करने में किस चीज़ की help लेंगे → Information Technology की → तो Auditor को set-up and organisation of IT Department की understanding लेनी होगी

(ii) Understanding the technology

The key understandings required are as follows:

(a) Analysis of business processes and Level of computerisation.

(b) Understanding technology architecture such as, it is distributed architecture, or a centralised Architecture or a hybrid architecture. eg: banks use primarily distributed architecture; i.e., process Data from Anywhere

(c) Assessing the Extent of ~~Dependance~~ Dependence of organisation on Information technology to Conduct business Activities. eg: banks are highly ~~dependant~~ dependant upon IT for day-to-day operations and survival of business.

(d) Understanding how organisation systems connect with other stakeholders such as vendors ~~Supply~~ (Supply Chain Management), customers (Customer Relationship management), employees (ERM) and the government.

(e) Studying Network diagrams to understand physical and Logical Network connectivity.

(f) Knowledge of various technologies, and their advantages and Limitations is a critical competence Requirement for the Auditor. For example, Knowledge of Encryption techniques, firewall, client/server and cloud computing helps for effective IS Audit

(g) And finally, studying Information Technology policies, Standards, guidelines and procedures.

* Hint to Learn :-

Technology से Related किन चीज़ों को Auditor को समझना है (understanding लेनी है) :

(a) सबसे पहले Business Process और Level of computerisation को समझना है

↓

अब Business process को चलाने के लिए क्या चाहिए ? → Technology

↓

(b) तो अब ये समझना है कि Technology Architecture

कौनसा है Entity में (i.e., ~~Dist~~ Distributed or Centralised or hybrid Architecture).

(c) फिर ये समझना है कि organisation Information Technology पर किस Extent तक Dependant है

↓

अब इस Dependance on IT को समझने के लिए Auditor को 2 चीजें समझनी होंगी:

↓

(d) Organisation systems कैसे connect होते हैं with other stake holders like vendors, customers, Employees, government.

(+)

(e) Organisation के अंदर Physical and Logical Network Connectivity कैसी है → इसको समझो और इसको समझने के लिए → Network Diagrams को study करो.

(f) अब इन सब Aspects को समझने के लिए Auditor को various Technologies, उनके Advantages and Limitations की knowledge लेनी होगी

(g) और साथ ही साथ IT policies, standards, guidelines and procedures को study करनी पड़ेगी।

(iii) Risk Assessment and Materiality

Risks can be differentiated as:

→ Control Risk
→ Inherent Risk
→ Detection Risk

* Hint to Learn:

C I D → को बोलो Types of Risks को पता लगाया जाए

C → Control Risk
I → Inherent Risk
D → Detection Risk

(iv) Understanding Internal control systems
(v) Legal considerations and Audit Standards

Do from Book → No Hint

→ IS Audit Procedures and Audit Evidence (Audit Documentation)

(Do from Book → No Hint)

Next topic

(6) Concurrent or Continuous and Embedded Audit Modules

(Do from Book → No Hint)

(i) An Integrated Test facility
(ii) The Snapshot technique
(iii) SCARF : System Control Audit Review file
(iv) ~~CIF~~ Continuous and Intermittent Simulation (CIS)
(v) Audit Hooks (This topic is given in ICAI Study Module and ICAI Practice Manual)

→ Audit Hooks (as written in study module issued by ICAI)

These are Audit routines that flag suspicious transactions. For Example, Internal Auditors at Insurance Company determined that their policy holder system was vulnerable to ~~fraud~~ fraud every time a policy holder changed his or her name or Address and then, subsequently withdrew funds from the policy. They devised a system of Audit hooks to tag records with a name or Address change. The Internal Audit department will Investigate these tagged records for detecting fraud. When Audit hooks are employed, Auditors can be informed of questionable transactions as soon as they occur.

This approach of real time notification displays a message on the Auditor's terminal.

→ Advantages of Concurrent Auditing techniques

(1) Comprehensive and Detailed Auditing
(2) Timely Audit
(3) Surprise Test capability
(4) Assess whether Information system meets the set objectives.
(5) Training for new users.

* Hint to Learn

Concurrent Auditing Techniques के ~~4~~ या Advantages हैं?

→ एक Auditor है जो हमेशा office में Late आता था

(1) तो एक दिन ↓ Comprehensive and Detailed Auditing करने के लिए

(2) ↓ office में Time पर आ जाता (Timely Audit)

(3) और वे ↓ Staff को बोला कि आज सुरप्राइज़ Surprise Test है (Surprise Test capability)

(4) ↓ अब Surprise Test में Auditor ने ये Assess किया whether ~~Inter~~ Information System meets the set objectives.

अब, ई Auditor को लगता that Information System is Not meeting the set objectives

(5) तो Auditor ने सोचा कि अब New users को Training देनी ही पड़ेगी (Training New users)

Auditor की Detail में Audit ~~[illegible]~~ → Concurrent Auditing Techniques → की जगह से ही कर सकता है → Hence, these are advantages of concurrent Auditing techniques.

→ Disadvantages or Limitations of Concurrent Auditing techniques

(1) Stable Application System
(2) Missing Audit trail
(3) Expert knowledge of Information System working
(4) Availability of Resources
(5) Involvement in System Development

* Hint to Learn

(1) अगर एक Stable Application System में
(2) Audit trail missing (लापता) हो जाए
(3) तो एक ऐसे Person को बुलाना पड़ता है जिसको Information System working की Expert knowledge हो
(4) अब उस Expert Person को सारे Resources 'Available करवाने पड़ते हैं (Availability of Resources)
(5) और उस Person को सारे Resources देकर System Development में Involve करवाना पड़ता है (Involvement in System Development)

अब क्योंकि 1 Stable Application system मिलना, Expert knowledge वाले Person का मिलना, सारे Resources का मिलना, etc. मुश्किल होता है इसलिए ये सारे Points → Limitations of concurrent Auditing techniques का part है

Next topic

(7) Audit trail controls

[Hint for this topic has already been included in chapter -3 Notes (protection of Information Systems) → (pg 60 in these Notes)]

(19) Application Controls

output controls

1. Maintaining log.
2. Spooling / queue mediation control
3. Controls over printing
4. Report Distribution
5. Secured Maintenance of sensitive printed output forms / records.

[Hint for this topic has already been included in Chapter 3 Notes (protection of Information Systems) → pg 59 in these Notes]

[PLEASE DO THE REST OF THE CHAPTER FROM BOOK]

CHAPTER-2

INFORMATION ~~SYSS~~ SYSTEM CONCEPTS

(Hint for only 3 topics is included here in these Notes)

→ Management INFORMATION SYSTEM (MIS)

Misconceptions about MIS

1. MIS is related only with computers
2. More Data Means More Information
3. Accuracy in Reporting is of prime importance

* Hint to Learn:

MIS से Related ~~तीन~~ Misconceptions हैं ?

① सबसे पहला Misconception ये है कि MIS सिर्फ computers से related है

↓

अत computers में होता है → Data

② तो दूसरा Misconception ये है कि ज्यादा Data मतलब ज्यादा Information.

↓

③ अब ये जो Data है → इसकी Reporting होती है

↓

④ तीसरा 3rd Misconception ये है कि Reporting में Accuracy को Prime Importance है

→ Pre-Requisites ~~Prerequisites~~ of an effective MIS

1. Support of Top Management
2. Qualified system and Management staff
3. Database
4. Control and Maintenance of MIS.
5. Evaluation of MIS.

* Hint to Learn

एक effective MIS के लिए कौनसे Prerequ Pre-requisites (Requirements) चाहिए होते हैं ?

① सबसे पहले तो MIS के लिए Top Management का support चाहिए

↓

② अब Top ~~Mang~~ Management के support से कौन दूसरा रहेगा → System and Manggement Staff.

→ and this staff should be qualified.

③

↓
अब इसे Top Management का support मिल जाया
(+) Qualified Staff भी आ जाया
↓
(3) तो अब मिलकर एक Database create करो जिसमें Data Maintained होगा → and such Database should be maintained in an integrated manner (Common Database)
↓
(4) इसके बाद organisation को controls apply करने होंगे → to ensure that everyone is following the same standard procedures (+) MIS की Maintenance का ध्यान रखना होगा, ie; changes/ Modifications should be there based on changing needs
(Control and Maintenance of MIS)
↓
(5) अब Last में हमें ये भी check करना होगा कि क्या MIS → Executives की Information Needs को ~~fulf~~ Fulfil कर पा रही है या नहीं (Evaluation of MIS)

→ Constraints in operating a Computer based MIS

Following are the major constraints in operating a computer based MIS:

(1) Non-Availability of Experts
(2) High turnover of experts.
(3) Lack of co-operation from staff
(4) Problem of selecting the sub-system of MIS to be installed and operated upon.
(5) No standardisation of MIS.
(6) Difficulty in quantifying the benefits of MIS.

* Hint to Learn:

क्या Major दिक्कतें आती हैं in operating a computer based MIS?

(1) सबसे पहली problem तो ये आती है कि हमें Experts नहीं मिलते (Non-Availability of Experts)
(2) अब अगर Experts मिल भी जाएँ तो भी There is a high-turnover of Experts (ie, Job-Switching)
(3) ऊपर से organisation का staff भी co-operate नहीं करता because of resistance to change, i.e., Non-Acceptance of computerised system.
(Lack of co-operation from staff)
(4) अगर ऊपर वाली problems solve हो भी जाएँ तो एक और problem है → हम select नहीं कर पाते उन first sub-systems को (i.e., Marketing, finance ya production) → जहाँ MIS can be installed and operated upon.
(5) और ~~सबसे~~ Main ~~problem~~ Problem of selecting the sub-system of MIS to be installed and operated upon)
(5) और सबसे main problem ये है कि MIS is a

Non- Standardised product, i.e., There is No standardisation of MIS
(Each organisation को अपनी Need के हिसाब से MIS की Requirement है)

(6) अब Last में organisation कहती है कि हमने इतनी परेशानी उठाई MIS को लाने के लिए → और अब हम ये सब Quantify नहीं कर पा रहे कि MIS के क्या Benefits हो रहे हैं. हमें because of Intangible Nature of Information Benefits.
(Difficulty in Quantifying the benefits of MIS).

(Please Do the Rest of the Chapter from Book)