Management Information & Control System

Keyur Shah

Starting Your Preparation for MICS:

If you are starting your preparation for MICS, high importantance wise chapter in exam is given below:

CHAPTER NO.	CHAPTER NAME	Rank	Page No
7	System Development Process	1	10
9	System's Acquisition, Software Development & Testing	2	17
13	General Controls in EDP Set-up	3	22
8	System Design	4	14
12	Enterprise Resource Planning – Redesigning Business	5	20
10	System Implementation & Maintenance	6	19
6	Enabling Technologies	7	8
18	Information Security	8	32
17	Audit of Information System	9	31
19	CASE Tools & Digital Technology	10	34
16	Cyber Laws & Information Technology Act, 2000	11	30
15	Detection of Computer Frauds	12	27
14	Application Controls in EDP Set-up	13	25
4	System's Approach & Decision Making	14	6
3	Basic Concepts of MIS	15	4
5	Decision Support & Executive Information System	16	7
1	Basic Concepts of System	17	2
2	Transaction Processing System	18	3

Basic Concept of System

1. Type of System

(1) Deterministic and Probabilistic System.
(2) Closed and Open System.

2. Characteristics of Information

(1) Timeliness
(2) Purpose
(3) Mode and Format
(4) Redundancy
(5) Rate
(6) Frequency
(7) Completeness
(8) Reliability
(9) Cost Benefit Analysis
(10) Validity
(11) Quality

3. Categories of Information Systems

(1) Transaction Processing System (TPS)
(2) Management Information System (MIS)
(3) Decision Support System (DSS)
(4) Executive Information System (EIS)
(5) Expert Systems (ES)

Transaction Processing System

1. Transaction Processing Cycle

1. Revenue Cycle
2. Expenditure Cycle
3. Production Cycle
4. Finance Cycle

2. Components of the Transaction Processing System

1 Inputs
2 Processing
3 Computer Storage
4 Computer Processing
5 Reference of Table File
6 Outputs

Basic Concept of MIS

1. Characteristics of an effective MIS

1. Management Oriented
2. Management Directed
3. Integrated
4. Common Data Flows
5. Heavy Planning Element
6. Sub System Concept
7. Common Database
8. Computerised

2. Misconception or Myths about MIS

1. The study of management information system is about the use of computers.
2. More data in reports means more information for managers.
3. Accuracy in reporting is of vital importance

3. Pre-Requisites of an effective MIS

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

4. Constrains in Operating a MIS

1. Non availability of Experts
2. Problem of selecting the sub-system
3. Varied objectives of business concerns
4. Non availability of Co-operation from staff
5. High turnover of Experts
6. Difficulty in Quantifying the benefit of MIS

5. Effects of using Computer for MIS

1. Speed of processing and retrieval of data increases
2. Scope of use of information system has expanded
3. Scope of analysis widened
4. Complexity of system design and operation increased
5. Integrates the working of different information sub-system
6. Increase the effectiveness of Information system
7. More comprehensive Information

6. Limitations of MIS

1. Quantity of Input and Processing
2. Not substitute for effective management only alternate tools for decision making
3. Not have requisite flexibility to quickly update itself
4. Can not provide tailor made information package
5. Ignore non-quantitative factors
6. Less useful for making non-programmed decisions
7. Less useful for non sharing culture organisations
8. Effectiveness decreases due to frequent changes in top-management, organizational structure and operation team

7. Establishing information requirement

1. Environment information
   (i) Government Policy
   (ii) Factors of Production
   (iii) Technological Environment
   (iv) Economic Trends
2. Competitive information
   (i) Industry demand
   (ii) Firm demand
   (iii) The Competitive Data
3. Internal information
   (i) Sales Forecast
   (ii) Financial Plan/Budget
   (iii) Supply Factors
   (iv) Internal Policies

8. Factors on which information requirements depend

1. Operational Function
2. Type of decision making
   (i) Programmed decisions
   (ii) Non-Programmed decision
3. Level of management activity
   (i) Strategic Level
   (ii) Tactical Level
   (iii) Supervisory Level

9. Levels of Management

1. Top Level (Strategic Level)
2. Middle Level (Tactical Level)
3. Supervisory Level

System approach and Decision Making

1. Step in the process of decision making

1. Defining of the problem
2. Gathering and analysing data concerning the problem
3. Identification of alternative solution
4. Evaluation of alternative solution
5. Selection of the best alternative
6. Implementation of the solution

2. Classification of Decisions

1. Programmed and non-programmed decisions
2. Strategic and Tactical decisions
3. Individual and Group decision

Decision Support and Executive Information Systems

1. Character of decision support system (DSS)

1. Semi structured and Un structured Decisions
2. Ability to adapt to changing needs
3. Easy to use

2. Components of Decision Support Systems (DSS)

1. The users
2. Databases
3. Planning Languages
4. Model Base

3. Tools of Decision Support Systems (DSS)

1. Data-based Software
2. Model Based Software
3. Statistical Software
4. Display Based Software

4. Characteristics of the types of information used in executive decision

1. Lack of Structure
2. High degree of uncertainty
3. Future Orientation
4. Informal source
5. Low Level of Detail

5. Purpose of Executive Information System

1. Support Managerial Learning
2. Timely access to information
3. Ability to direct management attention to specific areas

6. Principles to guide the design of measures and indicators to be included in an EIS

1. Easy to understand and collect.
2. Based on balanced view of the organization's objectives
3. Performance indicators
4. Encourage management and staff to share ownership of the organization's objectives
5. Provide everyone with useful information
6. Meet the changing needs of the organization.

Enabling Technologies

7. Traditional Computing Model

1. Mainframe Architecture
2. Personal Computers
3. File Sharing Architecture
4. Client Server Model

8. Benefit of the Client/Server Technology

1. Easier work
2. Reduction of Cost
3. Increase Productivity
4. End User Productivity
5. Developer Productivity
6. Less person required for maintenance
7. Less expenses in Hardware
8. Increase in Efficiency
9. Reduction in cost of purchasing, installing and upgrading software programs
10. Increase in Management control
11. Easier to implement
12. Long term cost benefits for development and support

9. Characteristics of Client/Server Technology

1. Consist of Client and Server process
2. Client and Server portion can operate on separate computer platforms
3. Any platform can be upgraded without having to upgrade the other platform
4. Server is able to service multiple clients or vise versa
5. Capability of networking
6. Significant portion of the application logic resides at the client end
7. Action is usually initiated at the client end
8. GUI generally resides at the client end
9. SQL capability is present
10. Database server should provide data protection and security

10. Components of Client Server Architecture

1. Client
2. Server
3. Middleware
4. Fat-client or Fat-Server
5. Network

11. Control techniques to increase the security as per IS auditor requirement

1. Disabling the floppy disk drive
2. Diskless workstation
3. Network monitoring
4. Data encryption techniques
5. Authentication system should be introduce by entering username and password
6. Use of Smart Card
7. Use of Application controls

12. Risk of Client/Server

1. Technological Risks
2. Operational Risks
3. Economic Risks
4. Political Risks

System Development Process

1. Activities of System Development Life Cycle

1. Preliminary Investigation
2. Requirements analysis or systems analysis
3. Design of System
4. Development of Software
5. Systems Testing
6. Implementation and Maintenance

2. Reason for failure system Development activities

1. Lack of senior management support for and involvement in information system development
2. Shifting user needs
3. Development of Strategic system
4. New Technologies
5. Lack of Standard Project management and systems development methodologies
6. Overworked or under-trained development staff
7. Resistance to change
8. Lack of user participation
9. Inadequate testing and user training

3. Approaches to Systems Development

1. Traditional Approach
2. Prototyping Approach
3. End user development approach
4. Top down Approach
5. Bottom up Approach
6. Systematic Approach for Development in small organizations

4. Steps for Prototyping Approach

1. Identify Information System Requirements
2. Develop the Initial Prototype
3. Test and Revise
4. Obtain User Signoff of the Approved Prototype

5. Advantage of Prototyping Approach

1. Satisfaction of users' needs and requirements
2. Short Period required for development
3. Errors detected and eliminated early in the developmental process

6. Disadvantage of Prototyping Approach

1. More time required in experimenting with approach
2. Frequently testing required
3. Cause behavioral problems with system users

7. Stages in Top down Approach

1. Analysis the objectives and goals of the organisation
2. Indentify the function of the organisation
3. Ascertain the major activities, decisions and functions
4. Indentify the information requirement for activities and decisions
5. Preparing specific information processing programs in detail and modules within these programs

8. Steps for Systematic Approach.

1. Indentify requirements
2. Locate, evaluate and secure suitable software
3. Locate, evaluate and secure suitable hardware
4. Implement the system

9. System Development Life Cycle Methodology

1. Project divided into number of identifiable processes
2. Periodically deliverables should be produced and monitors the development process
3. Requirement of Higher authority participate in project
4. Testing before implementation
5. Training plan should be develop for user
6. EDP Change Programme
7. Assess the effectiveness and efficiency before installing new system

10. Preliminary Investigation methodology/process

1. Definition of the scope of the study
2. Conducting the Investigation
3. Indentifying Viable Option
4. Testing Project's Feasibility
5. Estimating Costs and Benefits
6. Reporting Results to Management

11. Objectives of Preliminary Investigation

1. Clarify and understand the project request
2. Determine the size of the project
3. Technical and Operational feasibility
4. Assess cost benefits of alternative approaches
5. Report findings to the management

12. Methods of Investigation

1. Reviewing internal documents
2. Conducting interviews

13. Types of Project's Feasibility

1. Technical Feasibility
2. Economic Feasibility
3. Operational Feasibility
4. Schedule Feasibility
5. Legal Feasibility

14. Types of Cost in Cost benefit analysis

1. Development Cost
2. Operational Cost
3. Intangible Cost

15. Requirement Analysis Methodology

1. Fact Finding Technique
2. Analysis of the present system
3. System Analysis of Proposed System
4. Use of System development tools for system development

16. Fact finding techniques for systems analysis

1. Documents
2. Questionnaires
3. Interviews
4. Observation

17. Methods of analysis of Present system by the System Analyst

1. Review Historical Aspects
2. Analysis inputs
3. Review data files maintained
4. Review methods, procedures and data communications
5. Analyse outputs
6. Review internal controls
7. Model the existing physical system and logical system
8. Undertake overall analysis of present system

18. Tools for System Development

1. System Components and flows
2. User interface
3. Data attributes and relationships
4. Detailed system process

19. Tools of System Development

1. Flowchart
2. Data flow Diagram
3. Layout forms and screen
4. System components matrix
5. CASE Tools
6. Data Dictionary

20. Basic Elements for DFD

1. Data Sources and Dictionary
2. Data Flows
3. Processes
4. Data Stores

21. Information in Data Dictionary

1. Codes Describing Data
2. Sources Documents information
3. Name of Computer file
4. Computer programme name
5. Computer programme for file maintenance
6. Access the data items

System Design

1. Areas of New System Design

1. Output
2. Input
3. Processing
4. Storage
5. Procedures
6. Personnel

2. Important factors in Output design

1. Content
2. Form
3. Output Volume
4. Timeliness
5. Media
6. Format

3. Various methods of present output information

1. Tabular Format
2. Graphic Format

4. Guidelines for designing printed output

1. Read from left to right and top to bottom
2. Items should be easiest to find
3. Printed report should include heading, title of report, page number, etc
4. Related data should be grouped together
5. Control breaks should be used to find critical information
6. Sufficient margin should be made on page
7. Detail line for variable data should be defined
8. Mock up reports should be reviewed

5. Design of Visual Display

1. Physical dimensions of the screen
2. Number of rows and columns
3. Degree of Resolution
4. Number of Colours available
5. Methods of Highlighting
6. Methods of intensity control

6. Important factors for Input Design

1. Content
2. Timeliness
3. Media
4. Format
5. Input Volume

7. Guidelines for form Input design

1. Making forms easy to fill
   (i) Form Flow
   (ii) Divide forms in logical sections
   (iii) Filled Template
   (iv) Captioning
2. Meeting the intended purpose
3. Ensuring accurate completion
4. Keeping forms attractive

8. Coding methods for Input Design

1. Individuality
2. Space
3. Convenience
4. Expandability
5. Suggestiveness
6. Permanence

9. Coding Scheme for Input Design

1. Classification Codes
2. Function Codes
3. Significant-digit subset codes
4. Mnemonic Codes
5. Hierarchical Classification

10. Contains of System Manual

1. General Description of the existing system
2. Flow of existing system
3. Output of the existing system
4. General description of the new system
5. Flow of the new system
6. Output layout
7. Output distribution
8. Input layouts
9. Input responsibility
10. Macro-logic
11. Files to be maintained
12. List of Programs
13. Timing estimates
14. Controls
15. Audit Trail

System's Acquisition Software Development and Testing

1. Important points for selecting a computer system

1. Latest possible technology
2. Capability of Storage peripherals
3. Software Package
4. Compare same series computer
5. Vendor and machine selection

2. Advantage of Buying Software/Pre-written application package

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

3. Factors for validation of Vendors proposals evaluation

1. The performance Capability
2. The cost and benefit analysis
3. The Maintainability
4. The Compatibility
5. Vendor Support

4. Methods for Validation the vendors proposal

1. Checklists
2. Point-Scoring Analysis
3. Public evaluation reports

5. Stages for Software Development

1. Program Analysis
2. Program Design
3. Program Coding
4. Debug the program
   - (i) Use Structure walkthroughs
   - (ii) Test the program
   - (iii) Review the program code for adherence to standards
5. Program documentation
6. Program maintenance

6. Tools for Program Design

1. Program flow Chart
2. Pseudo Code
3. Structure Chart
4. 4GL Tools
5. Object oriented programming and design tools

7. Pre-requisite for system testing

1. Preparing realistic test data
2. Processing Test date
3. Through checking of the results
4. Reviewing the results

System Implementation and Maintenance

1. Steps for Equipment Installation

1. Site Preparation
2. Equipment Installation
3. Equipment check out

2. Strategies for converting from the old system to the new system

1. Direct Chang over
2. Parallel conversion
3. Gradual Conversion
4. Modular prototype conversion
5. Distributed conversion

3. Fundamentally activities before conversion of previous system to new information system

1. Procedure Conversion
2. File Conversion
3. System Conversion
4. Scheduling Personnel and equipment
5. Alternative plans in case of equipment failure

4. Types of evaluation of the new system

1. Development evaluation
2. Operation Evaluation
3. Information Evaluation

5. Category of System Maintenance

1. Schedule maintenance
2. Recue maintenance

Enterprise Resource Planning: redesigning Business

1. Characteristics of ERP

1. Flexibility
2. Modular & Open
3. Comprehensive
4. Beyond the Company
5. Best Business Practices

2. Features of ERP

1. ERP provided muliti-facility
2. Support Planning
3. End to end supply chain management
4. Company-wide integrated information system
5. Increase Corporate Goodwill
6. Became bridge the information gap across organisations
7. Integration of system
8. Solution for better project management
9. Allows automatic introduction of the latest technologies
10. Eliminates problem
11. Provides intelligent business tools

3. Benefits of ERP

1. Gives better business control
2. Reduce paper work
3. Improve timeliness
4. Faster customer response
5. Better monitoring and quicker resolution of queries
6. Quick response to changing market conditions
7. Competitive Advantage
8. Improve Supply-demand linkage
9. Improve international business
10. Better access of Management Information

4. Methodology for ERP Implementation

1. Indentifying the needs
2. Evaluation ERP
3. Deciding
4. Reengineering the business process
5. Evaluation various ERP Package
6. Finalising most suitable ERP Package
7. Installing the required hardware and software
8. Finalising consultants

9. Implementing the ERP Package

5. Criteria for evaluation various ERP package

1. Flexibility
2. Comprehensive
3. Integrated
4. Beyond the company
5. Best business practices
6. New technologies

6. Guidelines for ERP Implementation

1. Understanding the corporate needs and culture of the organization
2. Process redesign exercise
3. Establish good communication network
4. Provide strong and effective leadership
5. Finding an efficient and capable project manager
6. Creating a balanced team
7. Selecting a good implementation methodology
8. Training end user
9. Making the required changes in the working environment

Controls in EDP Set-Up: General Controls

1. Types of Controls in a Computer-Based systems

1. General Controls
2. Application Controls

2. Types of General Control

1. Operating system Controls
2. Data management Controls
3. Organizational structure Controls
4. System Development Controls
5. System Maintenance Controls
6. Computer Centre Security Controls
7. Internet and Intranet Controls
8. Personal Computer Controls

3. Objectives of Operating systems controls

1. Protect itself from users
2. Protect users from each others
3. Protect users from themselves
4. Protected from itself
5. Protected from its environment

4. Security Components for Operating System

1. Logon Procedure
2. Access Token
3. Access Control List
4. Discretionary Access Control

5. Threats to Operating System Integrity

1. Accidental Threats
2. Intentional Threats

6. Controlling Access Privileges for Operating system

1. Password Control
2. Reusable Passwords
3. One-time Passwords

7. List of Common type of Destructive Programs in Operating System

1. Virus
2. Worm
3. Logic Bomb
4. Back Door
5. Trojan Horse

8. Objective of Audit Trails to support security in Operating System

1. Detecting Unauthorized Access
2. Reconstructing Events
3. Personal Accountability

9. List of Several database control features

1. User View
2. Database Authorization Table
3. User-Defined Procedures
4. Data Encryption
5. Biometric Devices

10. Back Up Controls

1. The File Security
   (i) Magnetic Disk
   (ii) Magnetic Tape
2. Backup controls in the Database Environment

11. List controls in Organization Structure

1. Separating systems development from computers operations
2. Separating the database Administrator from other Functions
3. Separating New Systems Development from Maintenance
4. An Alternative Structure for Systems Development
5. Separating the Data Library from Operations

12. Activities of System development Controls

1. System Authorization Activities
2. User Specification Activities
3. Technical Design Activates
4. Internal Audit Participation
5. Program Testing
6. User Test and Acceptance Procedures

13. Activities of system Maintenance Controls

1. Maintenance Authorisation, Testing and Documentation
2. Source Program Library Controls
3. Audit Trail and Management Report
4. Program Version Number
5. Controlling Access to Maintenance Commands
6. Message Sequence Numbering

14. Various causes which damage Computer Centre Security

1. Fire Damage
2. Water Damage
3. Energy Variations
4. Pollution damage
5. Unauthorized Intrusion

15. Types of Internet Thereat

1. Invasive Tap
2. Inductive Tap

16. List of major features of well designed fire protection system

1. Automatic and manual Fire alarm
2. Fire System
3. Manual Fire Extinguisher at strategic location
4. Control Panel
5. Master Switches installed
6. Building may be constructed from fire resistant materials
7. Fire Extinguishers and Fire Exists should be marked clearly
8. Automated system should be installed to inform fire station
9. Experienced Security Office should be deployed

17. Components of Disaster Recovery Plan

1. Emergency Plan
2. Recovery Plan
3. Backup Plan
4. Test Plan

18. Tools for Controlling risk from Subversive Threats

1. Firewalls
   (i) Networks-Level Firewalls
   (ii) Application-level firewall
2. Controlling Denial of Service attacks
3. Encryption
   (i) Private Key Encryption
   (ii) Public Key Encryption
4. Message Transaction Log
5. Call Back Devices

19. Inherent Problems of Personal Computers and the Controls

1. Weak Access control
2. Multilevel Password Control
3. Inadequate Backup Procedure

Controls in EDP Set-UP: Application Controls

1. Classes of Input Control

1. Source Document Controls
2. Data Coding Controls
3. Batch Controls
4. Input error Correction
5. Generalized data input systems

2. Control List for Source Document

1. Use Pre numbered Source Documents
2. Use Source Documents in Sequence
3. Periodically Audit source Documents

3. Types of Error in Data coding control

1. Transcription Error
   - (i) Addition Error
   - (ii) Truncation Error
   - (iii) Substitution Error
2. Transposition Error
   - (i) Single Transpositions
   - (ii) Multiple Transposition

4. Levels of Input Validation Controls

1. Field Interrogation
2. Record Interrogation
3. File Interrogation

5. Common Type of Field Interrogation

1. Limit Checks
2. Picture Checks
3. Valid Code Checks
4. Check Digit
5. Arithmetic Checks
6. Cross Checks

6. Common Type of Record Interrogation

1. Sequence Checks
2. Format Completeness Checks
3. Redundant data checks
4. Combination Checks
5. Passwords

7. Common Type of File Interrogation

1. Internal Label Checks
2. Version Checks
3. An Expiration Date Checks

8. Common error-handling technique for input error correction

1. Immediate Correction
2. Create an error file
3. Reject the entire batch

9. Categories of Processing Controls

1. Run-to-Run Controls
2. Operator Intervention controls
3. Audit Trail Controls

10. Techniques to preserve audit trails in Computer Based Information System

1. Transaction Logs
2. Transaction Listing
3. Log of Automatic Transactions
4. Listing of Automatic Transactions
5. Unique Transaction Identifiers
6. Error Listing

11. Type of Output Control

1. Tape and Disk Output Controls
2. Printed Output Controls

12. Techniques of Output controls for printed output

1. Verification of Output
2. Distribution of Output
3. Procedures for acting on exception reports

Detection of Computer Frauds

1. Computers frauds include following activity

1. Clearly recognizable frauds
2. Hacking
3. Manipulation of computer system
4. Theft or destruction of confidential and sensitive information
5. Abuse of computer systems by employees
6. software piracy

2. Reason for Business take Computer fraud Seriously

1. Depend on network or stand alone computer
2. Link through computer networks
3. Business connected to the internet and more risk of hacking
4. Theft or destruction of electronic payments during transmission

3. Computer Fraud V/s Conventional Fraud

1. Easily hidden and hard to deduct
2. Evidence hard to find and difficult to present in the court
3. Easily Committed

4. Data Processing model fraud

1. Input
2. Processor
3. Computer Instruction
4. Data
5. Output
6. Malicious alterations of email

5. Reason for Increasing Computer Fraud

1. It is unregulated
2. Low Cost and can be set up anywhere in India
3. An impressive site
4. Glamour and novelty
5. May operate outside the legal jurisdiction

6. Reason for not knows how many companies loosed because of Computer Fraud

1. Not everyone agrees on what constitute computer fraud
2. Many computers frauds go undetected
3. Frauds are not reported
4. Most networks have a low level of security
5. Many internet pages give step by step instruction on how to perpetrate computer frauds and abuses
6. Law enforcement is unable to keep up with the growing number of computer frauds.

7. Precaution/measures for decrease the computer frauds

1. Make Fraud Less Likely to Occur
2. Use Proper Hiring and Firing Practices
3. Manage Disgruntled Employees
4. Train Employees in Security and Fraud Prevention Measures
   (i) Security measure
   (ii) Telephone disclosures
   (iii) Fraud awareness
   (iv) Ethical Considerations
   (v) Punishment for unethical behavior
   (vi) Educating employees in security issue
   (vii) Manage and Track Software Licenses
   (viii) Required Signed Confidentiality Agreements

8. Different way to control Computer fraud

1. Develop a Strong System of Internal Controls
2. Segregate Duties
3. Require Vacations and Rotate Duties
4. Restrict Access to Computer Equipment and Data Files
5. Encrypt Data and Programs
6. Protect Telephone Lines
7. Protect the System from Viruses
8. Control Sensitive Data
9. Control Laptop Computers

9. Steps to detect Computer Fraud

1. Conduct Frequent Audit
2. Use a Computer Security Officer
3. Use Computer Consultants
4. Monitor System Activates
5. Use fraud detection software

10. Methods to reduce Computer fraud Losses

1. Maintain Adequate Insurance
2. Keep a current backup copy
3. Develop a contingency plan
4. Use special software designed to monitor system activity

11. Reason for Fraud go undedicated.

1. Computer fraud are as yet undetected
2. Reluctant to report computer crimes
3. Courts are not much interested
4. Costly, time consuming to investigate
5. Lack of computer skills
6. Sentences are very light.

Cyber Laws and Information Technology Act 2000

1. Objectives of Act

1. To grant Legal Recognition for transaction
2. To give Legal Recognition to Digital Signature
3. To facilitate electronic filing of documents with Government
4. To facilitate electronic storage of data
5. To facilitate and give legal sanction to electronic fund transfer
6. To give legal recognition for keeping books of account by bankers
7. to amend the various Indian act

2. Areas where act shall not apply

1. A negotiable Instrument
2. A trust
3. A will
4. Any contract for the sale or conveyance of immovable property
5. Any such class of documents or transactions

Audit of Information Systems

1. Disadvantage of Computer Audit Approach

1. Electronic Evidence
2. Terminology
3. Automated Processes
4. New Risks and Controls
5. Reliance on Controls

2. Areas for review before starting of Information System (IS) audit

1. Computerised Systems and Applications
2. Information Processing Facilities
3. System Development
4. Management of Information systems
5. Client/Server, Telecommunications and Intranets

3. Framework for auditing computer security

1. Types of Security errors and Fraud faced by companies
2. Control Procedures to minimize security errors and fraud
3. Systems review audit procedures
4. Tests of controls audit procedures
5. Compensating Controls

Information Security

1. Objective of Information Security

1. Information easily available and usable when required (Availability)
2. Data and information are disclosed only to those who have a right to know it (Confidentiality)
3. Data and Information are protected against unauthorized modification (Integrity)

2. List of Critical Information

1. Strategic Plans
2. Business Operation
3. Finances

3. Step for establishing better information protection

1. Not all data has the same value
2. Know where the critical data resides
3. Develop an access control methodology
4. Protect information stored on media
5. Review hardcopy output

4. Core Principles of Security Objective

1. Accountability-Responsibility and accountability must be explicit
2. Awareness-Awareness of risks and security initiatives must be disseminated
3. Multidisciplinary-Security must be addressed taking into consideration both technological and non technological issues
4. Cost Effectiveness-Security must be cost effective
5. Integration-Security must be coordinated and integrated
6. Reassessment-Security must be reassessed periodically
7. Timeliness-Security procedures must provide for monitoring and timely response
8. Societal Factors- Ethics must be promoted by respecting the rights and interests of others.

5. Types of Protection for an Organization

1. Preventative Information Protection
2. Restorative Information Protection
3. Holistic Protection

6. Approach to implement Information Security

1. Securities Policy
2. Policy Development
3. Roles and Responsibilities
4. Design
5. Implementation
6. Monitoring
7. Awareness, Training and Education

7. Controls for Implementation

1. Managerial Controls
2. Identification and authentication controls
3. Logical access controls
4. Accountability Controls
5. Cryptography Controls
6. Systems development life cycle process controls
7. Physical and environmental controls
8. Business continuity planning controls

8. Role of Security Administrator

1. Safe from threats
2. Set Policy
3. Investigates and monitors pertaining to security
4. Responsible for establishing the minimal fixed requirements
5. Guides other information security
6. Other Duty
7. Possible of possible threats to the organization

Use of Simple CASE Tools, Analysis of Financial Statements using Digital Technology

1. Key components of Computer Aided Software Engineering (CASE) environments

1. Analysis Dimension
2. Development Dimension
3. Management Dimension
4. Support Dimension

2. Category of CASE Tools

1. Tools
2. Workbench
3. Environment Support

4. Levels of Integration of CASE Tools

1. Platform Integration
2. Data Integration
3. Presentation Integration
4. Control Integration
5. Process Integration

5. Types of CASE Work Benches

1. Programming work benches
2. 4GL work benches
3. Analysis and design work benches
4. Testing work benches
5. Meta-CASE work benches

6. Tools of Programming Work Benches

1. Language compiler
2. Structured Editor
3. Linker
4. Loader
5. Cross Referencer
6. Pretty printer
7. Static Analyser
8. Dynamic Analyser
9. Interactive debugger

7. Aspects to be considered in Meta-CASE Workbenches

1. A data model
2. A frame model
3. Diagrammatic notation
4. Textual presentation
5. Report Structures

8. Components of a CASE Work bench

1. A diagram editing system
2. Design analysis and checking facilities
3. Query language facilities
4. Data dictionary
5. Report generation
6. Forms generation
7. Import/Export Facilities
8. Some system support skeleton code generatioin

Exam Paper Analysis at a glance:

1. Compulsory Question

1. EDP General Controls (Ch 13)
2. EDP Application Controls (Ch 14)
3. Computer Frauds (Ch 15)
4. Cyber Laws (Ch 16)
5. Audit of Information System (Ch17)
6. MIS (Ch.3)

2. Normal Questions with high value

1. System Development Process (Ch7)
2. System Design (Ch 8)
3. System Acquisition S/W Development & Testing(Ch 9)
4. System Implementation & Maintenance (Ch 10)
5. Design of Computerised Commercial Applications (Ch 11)
6. Information Security (Ch 18)

3 Less Important Chapters

1. Basic Concept of Systems (Ch1)
2. System Approach & Decision Making(Ch 4)
3. Decision Support System (Ch 5)
4. Enabling Technologies (Ch 6)
5. ERP (Ch 12)
6. CASE Tools (Ch 19)

4. Other points to remember

1. As per the analysis for last several exam papers Chapter 7 to Chapter 10 (System Development to System Maintenance) comes for nearly 40-45 marks.
2. Questions from Design of Computerised Commercial Applications (Ch 11). This Question will always come directly from institute Module.
3. Do not leave MIS. Last few papers there is high weight around 15 Marks.
4. Also EDP General & EDP Application Controls comes for around 15-25 Marks and it mostly comes along with Fraud or System Chapters 7 to 10.