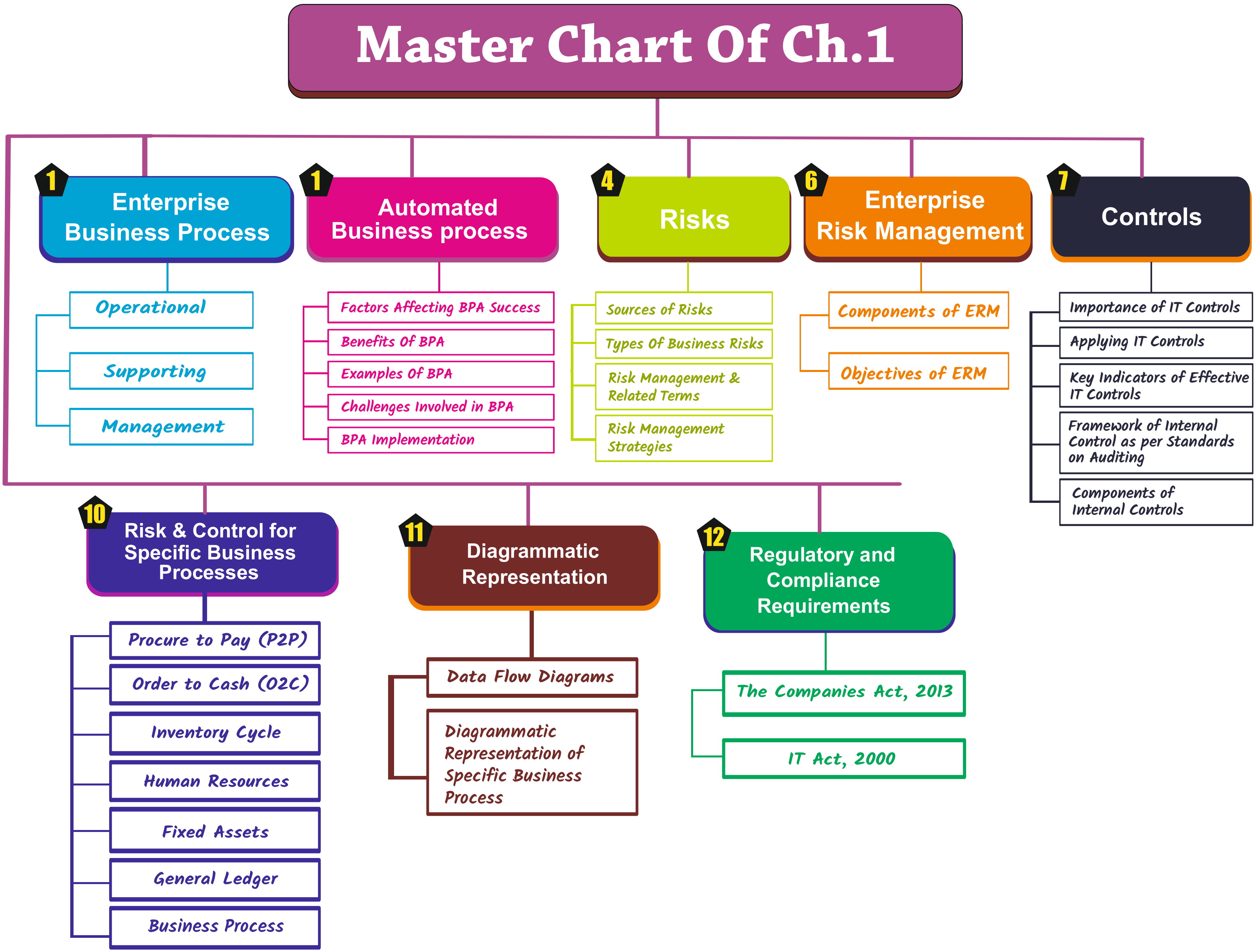
Master Chart Of Ch.1



1 Enterprise Business Process

- Operational
- Supporting
- Management

1 Automated Business process

- Factors Affecting BPA Success
- Benefits Of BPA
- Examples Of BPA
- Challenges Involved in BPA
- BPA Implementation

4 Risks

- Sources of Risks
- Types Of Business Risks
- Risk Management & Related Terms
- Risk Management Strategies

6 Enterprise Risk Management

- Components of ERM
- Objectives of ERM

7 Controls

- Importance of IT Controls
- Applying IT Controls
- Key Indicators of Effective IT Controls
- Framework of Internal Control as per Standards on Auditing
- Components of Internal Controls

10 Risk & Control for Specific Business Processes

- Procure to Pay (P2P)
- Order to Cash (O2C)
- Inventory Cycle
- Human Resources
- Fixed Assets
- General Ledger
- Business Process

11 Diagrammatic Representation

- Data Flow Diagrams
- Diagrammatic Representation of Specific Business Process

12 Regulatory and Compliance Requirements

- The Companies Act, 2013
- IT Act, 2000

Master Chart of Ch.2

19 INTEGRATED (ERP) AND NON-INTEGRATED SYSTEMS

a) What is a System?

b) What is a Process?

c) Concepts in Computerized Accounting Systems

- Types of Data
- Voucher Types
- Voucher Number
- Accounting Flow
- Types of Ledgers
- Grouping of Ledgers

d) Technical Concepts

- Working of any software
- Installed Applications V/s Web Applications

e) Non-Integrated System

f) Enterprise Resource Planning (ERP) Systems

g) Benefits of an ERP Systems

23 Risks And Controls in an ERP Environment

a) ERP Implementation Its Risk & Related Controls

b) Role Based Access Control (RBAC) in ERP System

c) Types of Access

24 Business Process Modules And Their Integration With Financial & Accounting Systems

a) What is a Business Process?

b) Business Process Flow

c) Integration with Other Modules

d) Business Categories of BPM

e) Functional Modules of ERP

34 Applicable Regulatory & Compliance Requirements

a) What is Regulatory Compliance?

b) Pros and Cons of having single software for Accounting and Tax Compliance

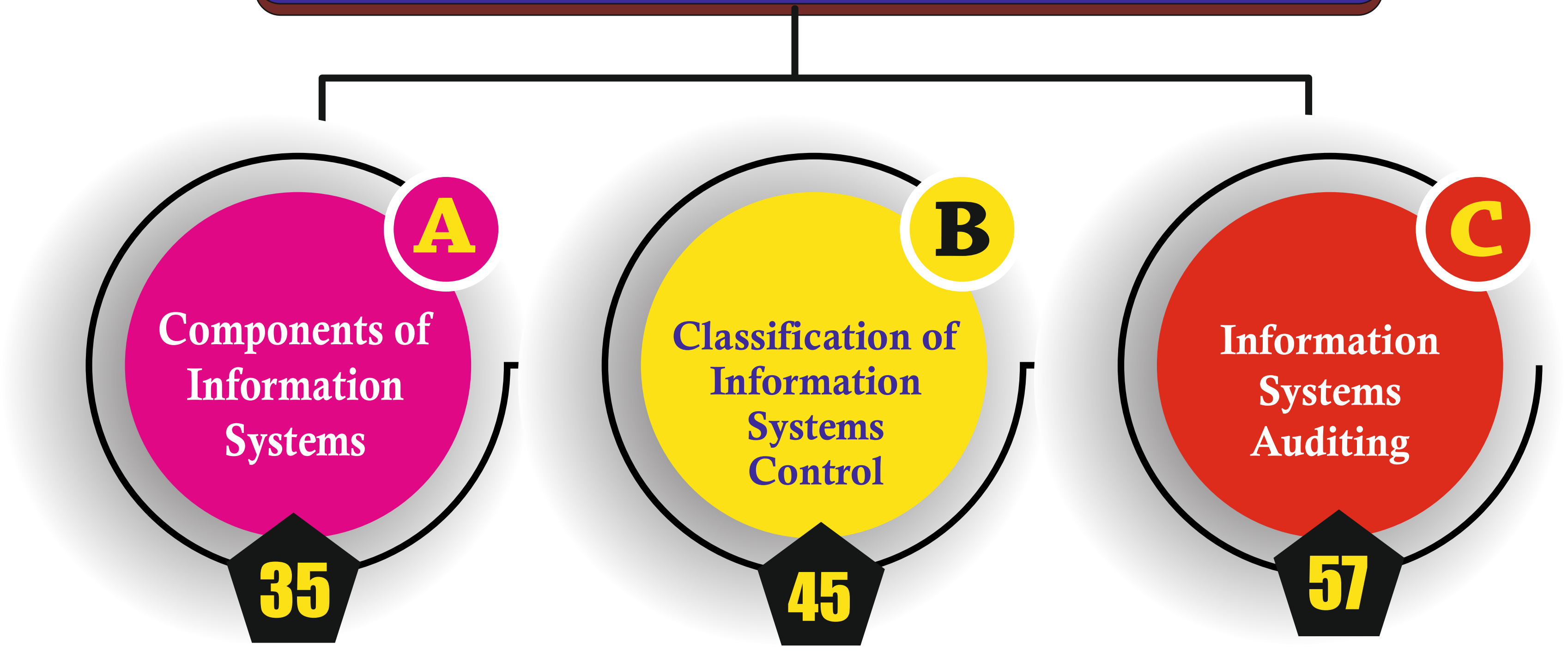
24 Audit Of Erp Systems

29 Reporting System And Management Information Systems (MIS)

30 Data Analytics And Business Intelligence

32 Business Reporting And Fundamentals Of Xbrl

Master Chart of ch.3



A

Components of Information Systems

35

B

Classification of Information Systems Control

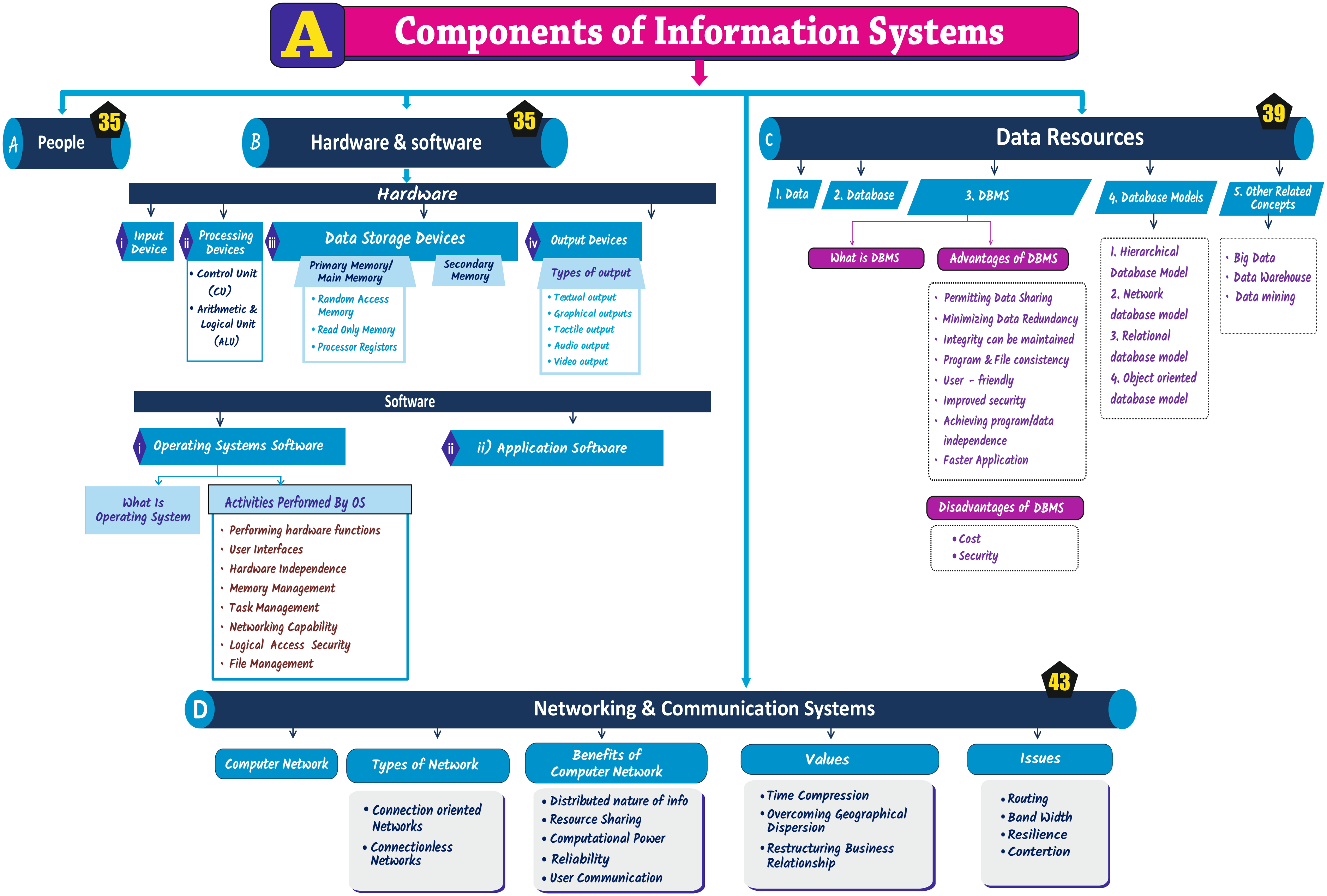
45

C

Information Systems Auditing

57

A Components of Information Systems



A People 35

B Hardware & software 35

Hardware

- i Input Device
- ii Processing Devices
  - Control Unit (CU)
  - Arithmetic & Logical Unit (ALU)
- iii Data Storage Devices
  - Primary Memory/ Main Memory
    - Random Access Memory
    - Read Only Memory
    - Processor Registors
  - Secondary Memory
- iv Output Devices
  - Types of output
    - Textual output
    - Graphical outputs
    - Tactile output
    - Audio output
    - Video output

Software

- i Operating Systems Software
  - What Is Operating System
  - Activities Performed By OS
    - Performing hardware functions
    - User Interfaces
    - Hardware Independence
    - Memory Management
    - Task Management
    - Networking Capability
    - Logical Access Security
    - File Management
- ii ii) Application Software

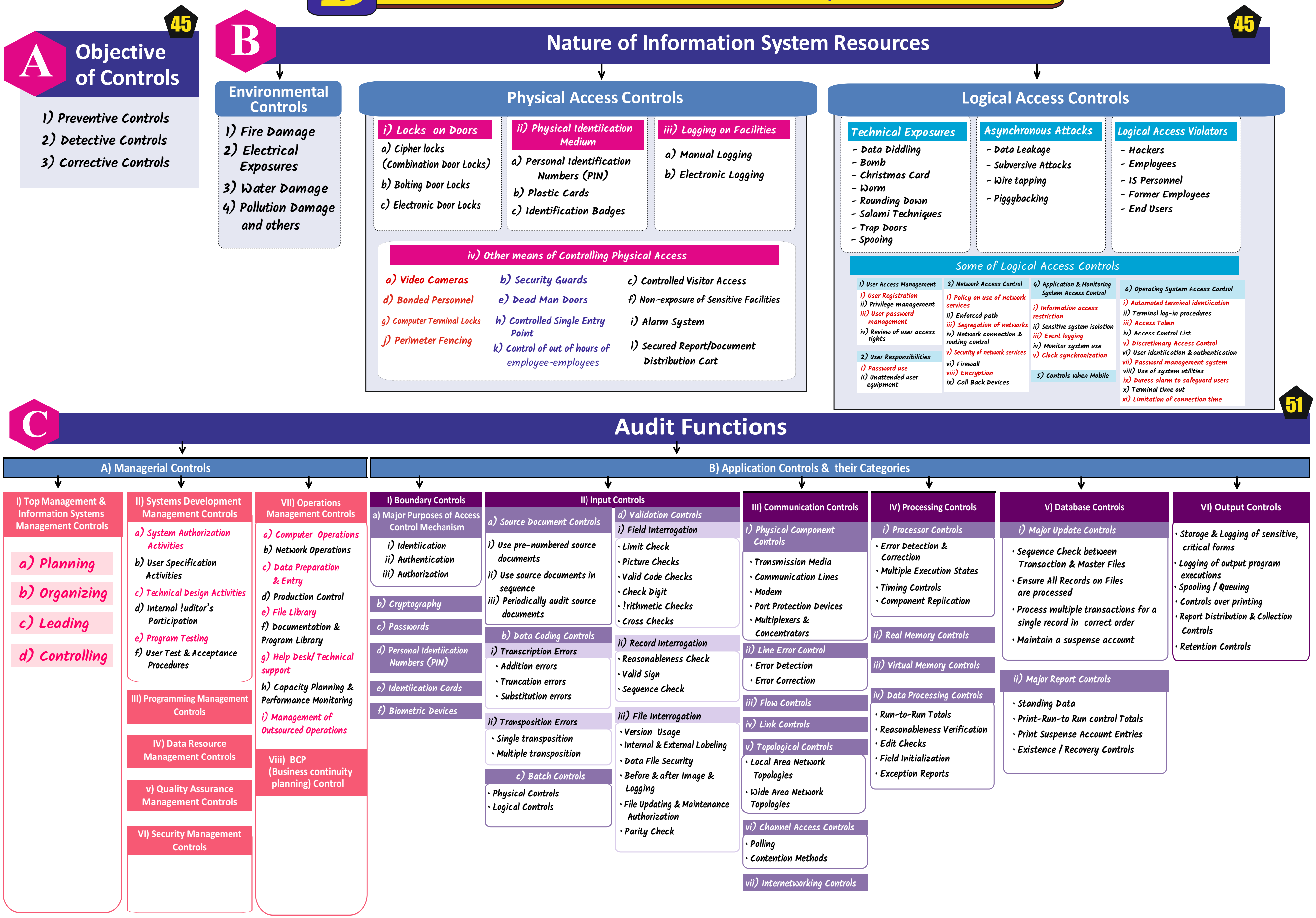
C Data Resources 39

- 1. Data
- 2. Database
- 3. DBMS
  - What is DBMS
  - Advantages of DBMS
    - Permitting Data Sharing
    - Minimizing Data Redundancy
    - Integrity can be maintained
    - Program & File consistency
    - User - friendly
    - Improved security
    - Achieving program/data independence
    - Faster Application
  - Disadvantages of DBMS
    - Cost
    - Security
- 4. Database Models
  - 1. Hierarchical Database Model
  - 2. Network database model
  - 3. Relational database model
  - 4. Object oriented database model
- 5. Other Related Concepts
  - Big Data
  - Data Warehouse
  - Data mining

D Networking & Communication Systems 43

- Computer Network
- Types of Network
  - Connection oriented Networks
  - Connectionless Networks
- Benefits of Computer Network
  - Distributed nature of info
  - Resource Sharing
  - Computational Power
  - Reliability
  - User Communication
- Values
  - Time Compression
  - Overcoming Geographical Dispersion
  - Restructuring Business Relationship
- Issues
  - Routing
  - Band Width
  - Resilience
  - Contention

B Classification of Information Systems Control



45

A Objective of Controls

1) Preventive Controls
2) Detective Controls
3) Corrective Controls

B Nature of Information System Resources

45

Environmental Controls

1) Fire Damage
2) Electrical Exposures
3) Water Damage
4) Pollution Damage and others

Physical Access Controls

i) Locks on Doors

a) Cipher locks (Combination Door Locks)
b) Bolting Door Locks
c) Electronic Door Locks

ii) Physical Identiication Medium

a) Personal Identification Numbers (PIN)
b) Plastic Cards
c) Identification Badges

iii) Logging on Facilities

a) Manual Logging
b) Electronic Logging

iv) Other means of Controlling Physical Access

a) Video Cameras
b) Security Guards
c) Controlled Visitor Access
d) Bonded Personnel
e) Dead Man Doors
f) Non-exposure of Sensitive Facilities
g) Computer Terminal Locks
h) Controlled Single Entry Point
i) Alarm System
j) Perimeter Fencing
k) Control of out of hours of employee-employees
l) Secured Report/Document Distribution Cart

Logical Access Controls

Technical Exposures

- Data Diddling
- Bomb
- Christmas Card
- Worm
- Rounding Down
- Salami Techniques
- Trap Doors
- Spooing

Asynchronous Attacks

- Data Leakage
- Subversive Attacks
- Wire tapping
- Piggybacking

Logical Access Violators

- Hackers
- Employees
- IS Personnel
- Former Employees
- End Users

Some of Logical Access Controls

1) User Access Management

i) User Registration
ii) Privilege management
iii) User password management
iv) Review of user access rights

2) User Responsibilities

i) Password use
ii) Unattended user equipment

3) Network Access Control

i) Policy on use of network services
ii) Enforced path
iii) Segregation of networks
iv) Network connection & routing control
v) Security of network services
vi) Firewall
viii) Encryption
ix) Call Back Devices

4) Application & Monitoring System Access Control

i) Information access restriction
ii) Sensitive system isolation
iii) Event logging
iv) Monitor system use
v) Clock synchronization

5) Controls when Mobile

6) Operating System Access Control

i) Automated terminal identiication
ii) Terminal log-in procedures
iii) Access Token
iv) Access Control List
v) Discretionary Access Control
vi) User identiication & authentication
vii) Password management system
viii) Use of system utilities
ix) Duress alarm to safeguard users
x) Terminal time out
xi) Limitation of connection time

C Audit Functions

51

A) Managerial Controls

I) Top Management & Information Systems Management Controls

a) Planning
b) Organizing
c) Leading
d) Controlling

II) Systems Development Management Controls

a) System Authorization Activities
b) User Specification Activities
c) Technical Design Activities
d) Internal !uditor's Participation
e) Program Testing
f) User Test & Acceptance Procedures

III) Programming Management Controls

IV) Data Resource Management Controls

v) Quality Assurance Management Controls

VI) Security Management Controls

VII) Operations Management Controls

a) Computer Operations
b) Network Operations
c) Data Preparation & Entry
d) Production Control
e) File Library
f) Documentation & Program Library
g) Help Desk/ Technical support
h) Capacity Planning & Performance Monitoring
i) Management of Outsourced Operations

Viii) BCP (Business continuity planning) Control

B) Application Controls & their Categories

I) Boundary Controls

a) Major Purposes of Access Control Mechanism

i) Identiication
ii) Authentication
iii) Authorization

b) Cryptography

c) Passwords

d) Personal Identiication Numbers (PIN)

e) Identiication Cards

f) Biometric Devices

II) Input Controls

a) Source Document Controls

i) Use pre-numbered source documents
ii) Use source documents in sequence
iii) Periodically audit source documents

b) Data Coding Controls

i) Transcription Errors

- Addition errors
- Truncation errors
- Substitution errors

ii) Transposition Errors

- Single transposition
- Multiple transposition

c) Batch Controls

- Physical Controls
- Logical Controls

d) Validation Controls

i) Field Interrogation

- Limit Check
- Picture Checks
- Valid Code Checks
- Check Digit
- !rithmetic Checks
- Cross Checks

ii) Record Interrogation

- Reasonableness Check
- Valid Sign
- Sequence Check

iii) File Interrogation

- Version Usage
- Internal & External Labeling
- Data File Security
- Before & after Image & Logging
- File Updating & Maintenance Authorization
- Parity Check

III) Communication Controls

I) Physical Component Controls

- Transmission Media
- Communication Lines
- Modem
- Port Protection Devices
- Multiplexers & Concentrators

ii) Line Error Control

- Error Detection
- Error Correction

iii) Flow Controls

iv) Link Controls

v) Topological Controls

- Local Area Network Topologies
- Wide Area Network Topologies

vi) Channel Access Controls

- Polling
- Contention Methods

vii) Internetworking Controls

IV) Processing Controls

i) Processor Controls

- Error Detection & Correction
- Multiple Execution States
- Timing Controls
- Component Replication

ii) Real Memory Controls

iii) Virtual Memory Controls

iv) Data Processing Controls

- Run-to-Run Totals
- Reasonableness Verification
- Edit Checks
- Field Initialization
- Exception Reports

V) Database Controls

i) Major Update Controls

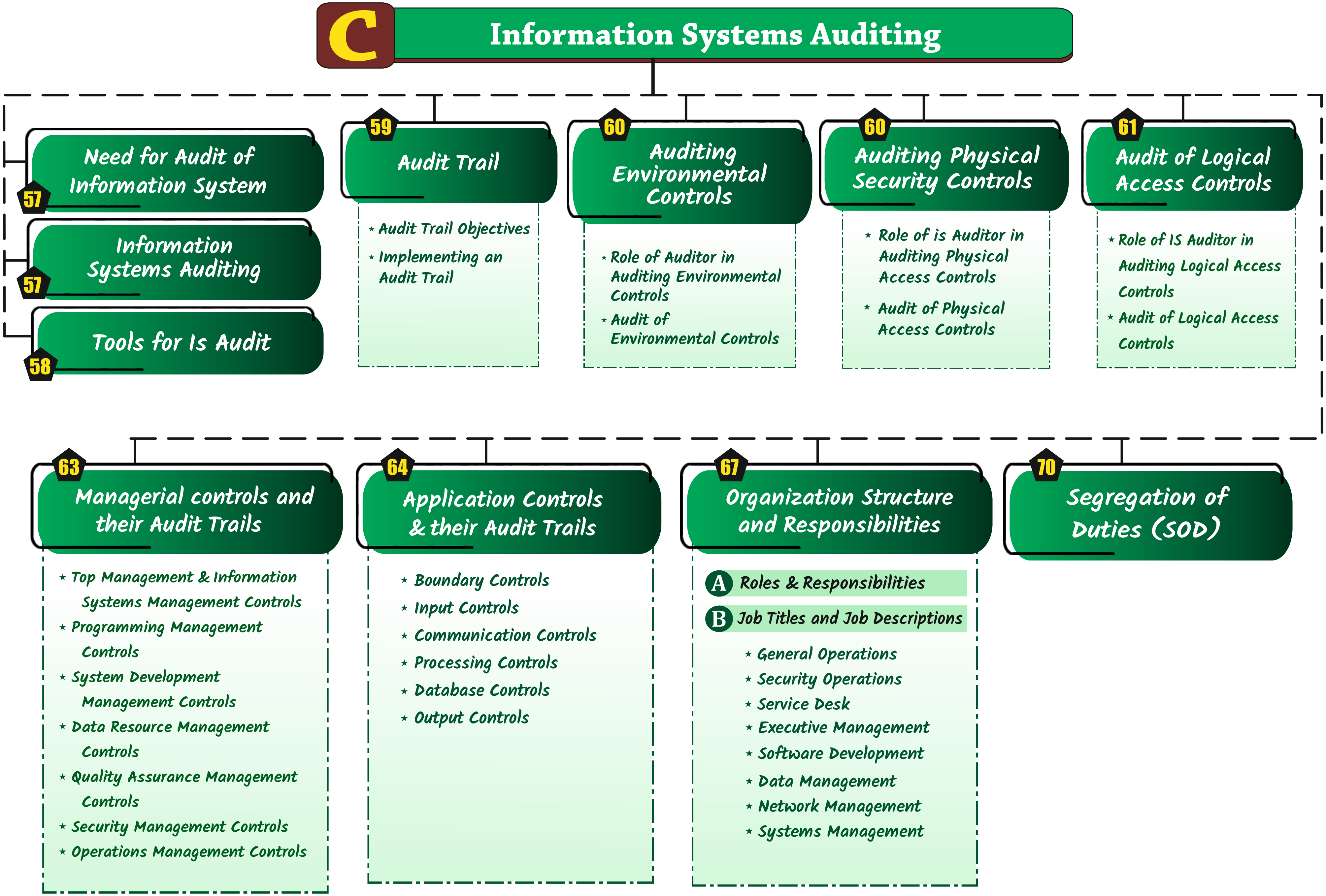
- Sequence Check between Transaction & Master Files
- Ensure All Records on Files are processed
- Process multiple transactions for a single record in correct order
- Maintain a suspense account

ii) Major Report Controls

- Standing Data
- Print-Run-to Run control Totals
- Print Suspense Account Entries
- Existence / Recovery Controls

VI) Output Controls

- Storage & Logging of sensitive, critical forms
- Logging of output program executions
- Spooling / Queuing
- Controls over printing
- Report Distribution & Collection Controls
- Retention Controls



C Information Systems Auditing

57 Need for Audit of Information System

57 Information Systems Auditing

58 Tools for Is Audit

59 Audit Trail

- Audit Trail Objectives
- Implementing an Audit Trail

60 Auditing Environmental Controls

- Role of Auditor in Auditing Environmental Controls
- Audit of Environmental Controls

60 Auditing Physical Security Controls

- Role of is Auditor in Auditing Physical Access Controls
- Audit of Physical Access Controls

61 Audit of Logical Access Controls

- Role of IS Auditor in Auditing Logical Access Controls
- Audit of Logical Access Controls

63 Managerial controls and their Audit Trails

- Top Management & Information Systems Management Controls
- Programming Management Controls
- System Development Management Controls
- Data Resource Management Controls
- Quality Assurance Management Controls
- Security Management Controls
- Operations Management Controls

64 Application Controls & their Audit Trails

- Boundary Controls
- Input Controls
- Communication Controls
- Processing Controls
- Database Controls
- Output Controls

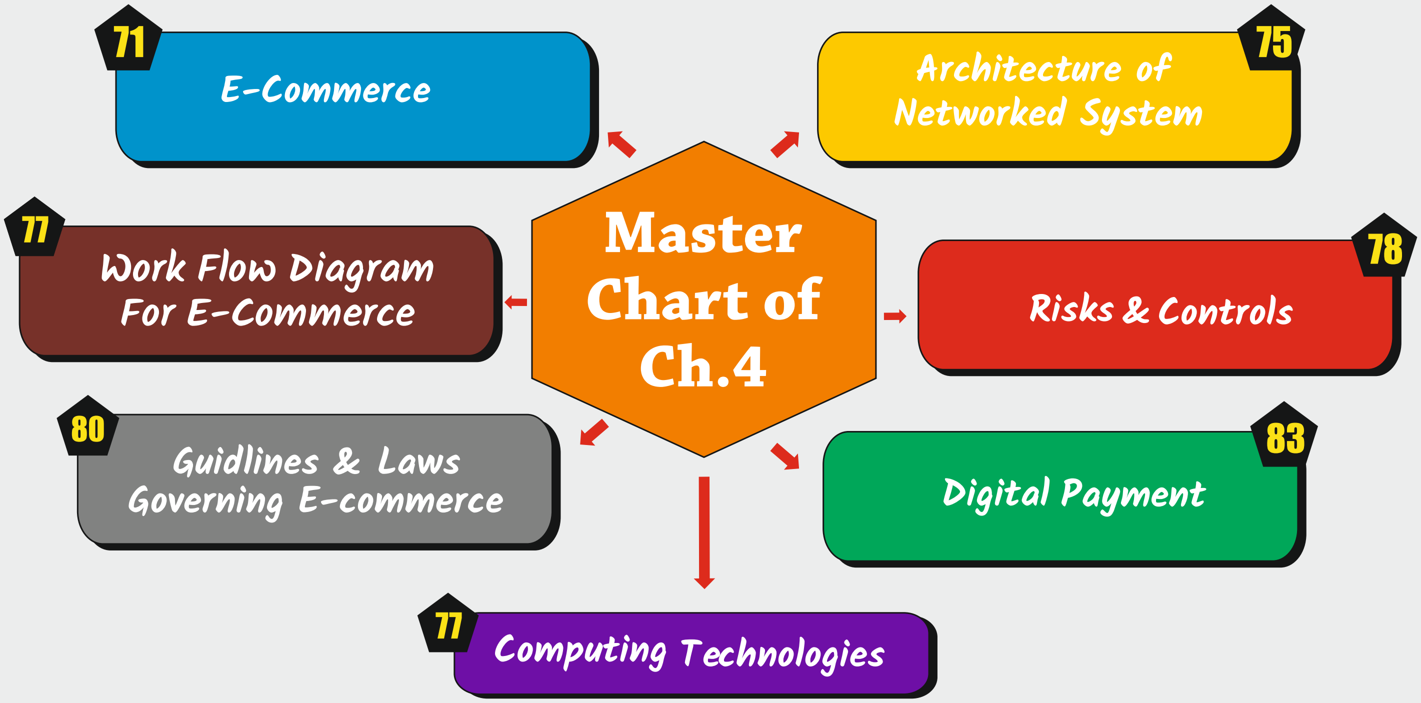
67 Organization Structure and Responsibilities

A Roles & Responsibilities

B Job Titles and Job Descriptions

- General Operations
- Security Operations
- Service Desk
- Executive Management
- Software Development
- Data Management
- Network Management
- Systems Management

70 Segregation of Duties (SOD)



Master Chart of Ch.4

71 E-Commerce

75 Architecture of Networked System

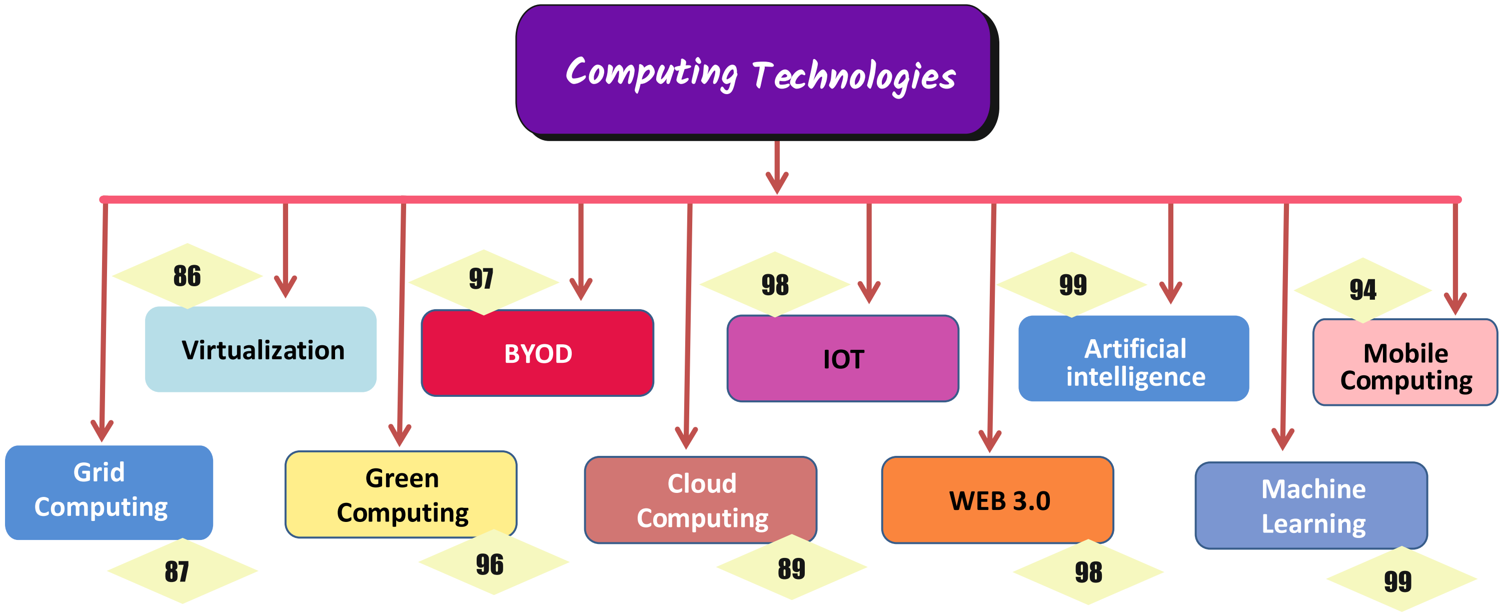
77 Work Flow Diagram For E-Commerce

78 Risks & Controls

80 Guidlines & Laws Governing E-commerce

83 Digital Payment

77 Computing Technologies



Computing Technologies

Grid Computing 87

86 Virtualization

Green Computing 96

97 BYOD

Cloud Computing 89

98 IOT

WEB 3.0 98

99 Artificial intelligence

Machine Learning 99

94 Mobile Computing

Master Chart of Ch 5

A — OVERVIEW OF BANKING SERVICES (100)

- Introduction
- Overview of Core Banking Systems

B — COMPONENT AND ARCHITECTURE OF CBS (102)

- Technology Components of CBS
- CBS IT Environment
- Functional Architecture Of CBS
- Internet Banking Process
- E-Commerce Transaction Processing

C — CBS RISKS, SECURITY POLICY AND CONTROLS (106)

- Risks Associated with CBS
- Security Policy
- Internal Control System in Bank
- CBS :
  Core Business Processes
  - Relevant Risks & Controls

D — APPLICABLE REGULATORY AND COMPLIANCE REQUIREMENTS (115)

- Impact of Technology in Banking
- Money Laundering
- Cyber Crimes
- Banking Regulation Acts