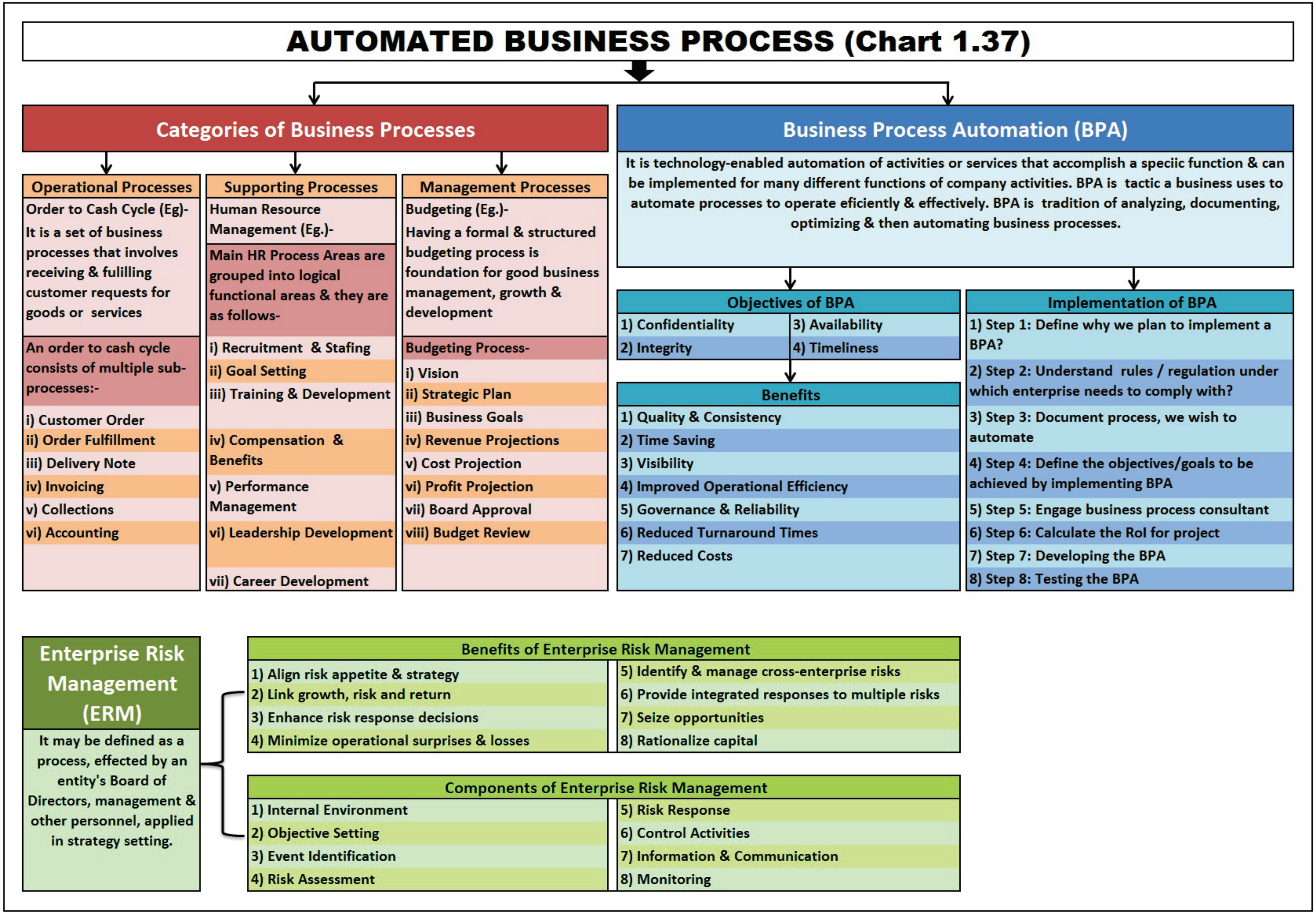


AUTOMATED BUSINESS PROCESS (Chart 1.37)

Categories of Business Processes

Operational Processes

Order to Cash Cycle (Eg)-

It is a set of business processes that involves receiving & fulilling customer requests for goods or services

An order to cash cycle consists of multiple sub-processes:-

i) Customer Order

ii) Order Fulfillment

iii) Delivery Note

iv) Invoicing

v) Collections

vi) Accounting

Supporting Processes

Human Resource Management (Eg.)-

Main HR Process Areas are grouped into logical functional areas & they are as follows-

i) Recruitment & Stafing

ii) Goal Setting

iii) Training & Development

iv) Compensation & Benefits

v) Performance Management

vi) Leadership Development

vii) Career Development

Management Processes

Budgeting (Eg.)-

Having a formal & structured budgeting process is foundation for good business management, growth & development

Budgeting Process-

i) Vision

ii) Strategic Plan

iii) Business Goals

iv) Revenue Projections

v) Cost Projection

vi) Profit Projection

vii) Board Approval

viii) Budget Review

Business Process Automation (BPA)

It is technology-enabled automation of activities or services that accomplish a speciic function & can be implemented for many different functions of company activities. BPA is tactic a business uses to automate processes to operate eficiently & effectively. BPA is tradition of analyzing, documenting, optimizing & then automating business processes.

Objectives of BPA

1) Confidentiality	3) Availability
2) Integrity	4) Timeliness

Benefits

1) Quality & Consistency

2) Time Saving

3) Visibility

4) Improved Operational Efficiency

5) Governance & Reliability

6) Reduced Turnaround Times

7) Reduced Costs

Implementation of BPA

1) Step 1: Define why we plan to implement a BPA?

2) Step 2: Understand rules / regulation under which enterprise needs to comply with?

3) Step 3: Document process, we wish to automate

4) Step 4: Define the objectives/goals to be achieved by implementing BPA

5) Step 5: Engage business process consultant

6) Step 6: Calculate the RoI for project

7) Step 7: Developing the BPA

8) Step 8: Testing the BPA

Enterprise Risk Management (ERM)

It may be defined as a process, effected by an entity's Board of Directors, management & other personnel, applied in strategy setting.

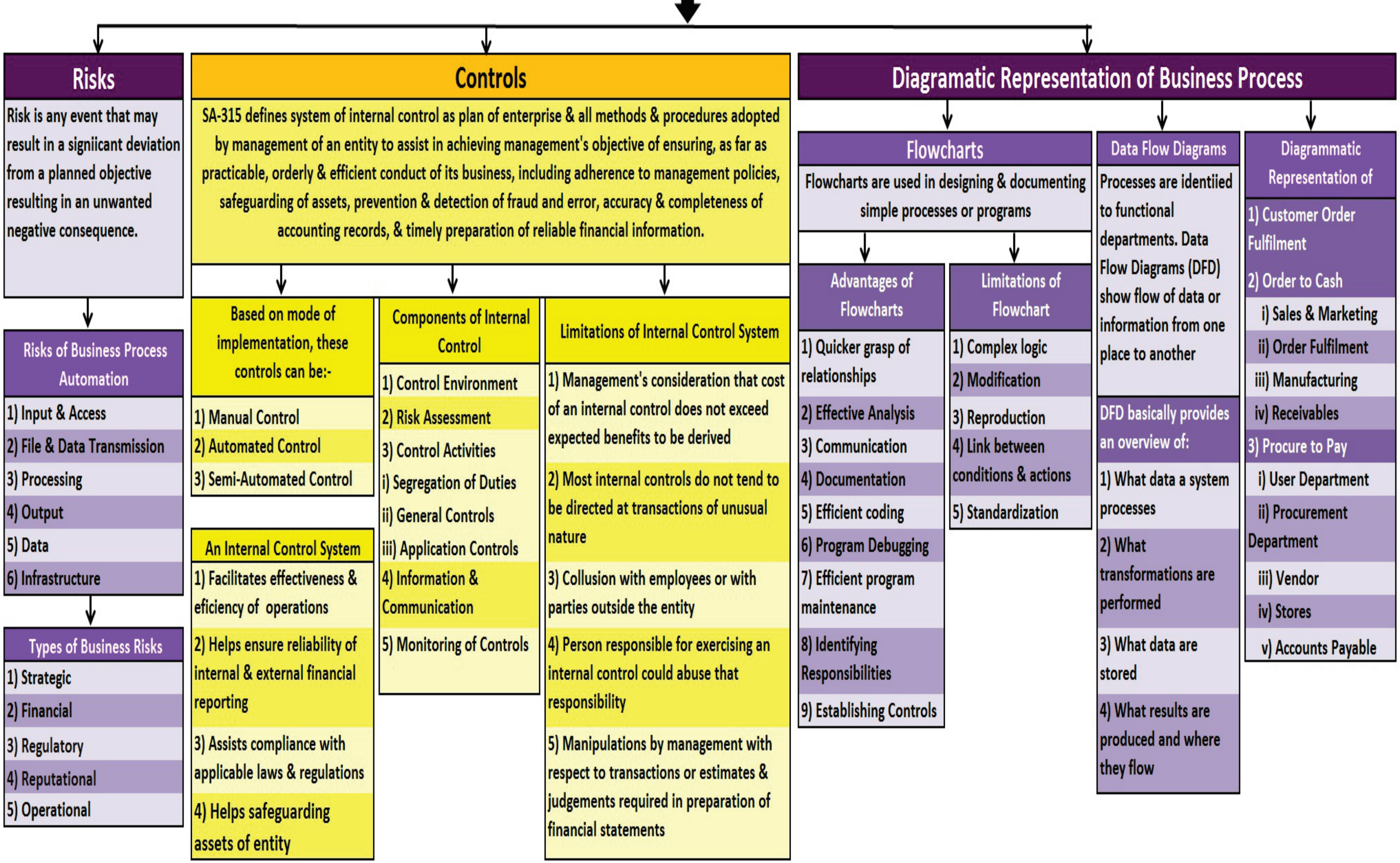
Benefits of Enterprise Risk Management

1) Align risk appetite & strategy	5) Identify & manage cross-enterprise risks
2) Link growth, risk and return	6) Provide integrated responses to multiple risks
3) Enhance risk response decisions	7) Seize opportunities
4) Minimize operational surprises & losses	8) Rationalize capital

Components of Enterprise Risk Management

1) Internal Environment	5) Risk Response
2) Objective Setting	6) Control Activities
3) Event Identification	7) Information & Communication
4) Risk Assessment	8) Monitoring

AUTOMATED BUSINESS PROCESS (Chart 1.38)



Risks

Risk is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence.

Risks of Business Process Automation

1) Input & Access
2) File & Data Transmission
3) Processing
4) Output
5) Data
6) Infrastructure

Types of Business Risks

1) Strategic
2) Financial
3) Regulatory
4) Reputational
5) Operational

Controls

SA-315 defines system of internal control as plan of enterprise & all methods & procedures adopted by management of an entity to assist in achieving management's objective of ensuring, as far as practicable, orderly & efficient conduct of its business, including adherence to management policies, safeguarding of assets, prevention & detection of fraud and error, accuracy & completeness of accounting records, & timely preparation of reliable financial information.

Based on mode of implementation, these controls can be:-

1) Manual Control
2) Automated Control
3) Semi-Automated Control

An Internal Control System

1) Facilitates effectiveness & efficiency of operations
2) Helps ensure reliability of internal & external financial reporting
3) Assists compliance with applicable laws & regulations
4) Helps safeguarding assets of entity

Components of Internal Control

1) Control Environment
2) Risk Assessment
3) Control Activities
i) Segregation of Duties
ii) General Controls
iii) Application Controls
4) Information & Communication
5) Monitoring of Controls

Limitations of Internal Control System

1) Management's consideration that cost of an internal control does not exceed expected benefits to be derived
2) Most internal controls do not tend to be directed at transactions of unusual nature
3) Collusion with employees or with parties outside the entity
4) Person responsible for exercising an internal control could abuse that responsibility
5) Manipulations by management with respect to transactions or estimates & judgements required in preparation of financial statements

Diagramatic Representation of Business Process

Flowcharts

Flowcharts are used in designing & documenting simple processes or programs

Advantages of Flowcharts

1) Quicker grasp of relationships
2) Effective Analysis
3) Communication
4) Documentation
5) Efficient coding
6) Program Debugging
7) Efficient program maintenance
8) Identifying Responsibilities
9) Establishing Controls

Limitations of Flowchart

1) Complex logic
2) Modification
3) Reproduction
4) Link between conditions & actions
5) Standardization

Data Flow Diagrams

Processes are identified to functional departments. Data Flow Diagrams (DFD) show flow of data or information from one place to another

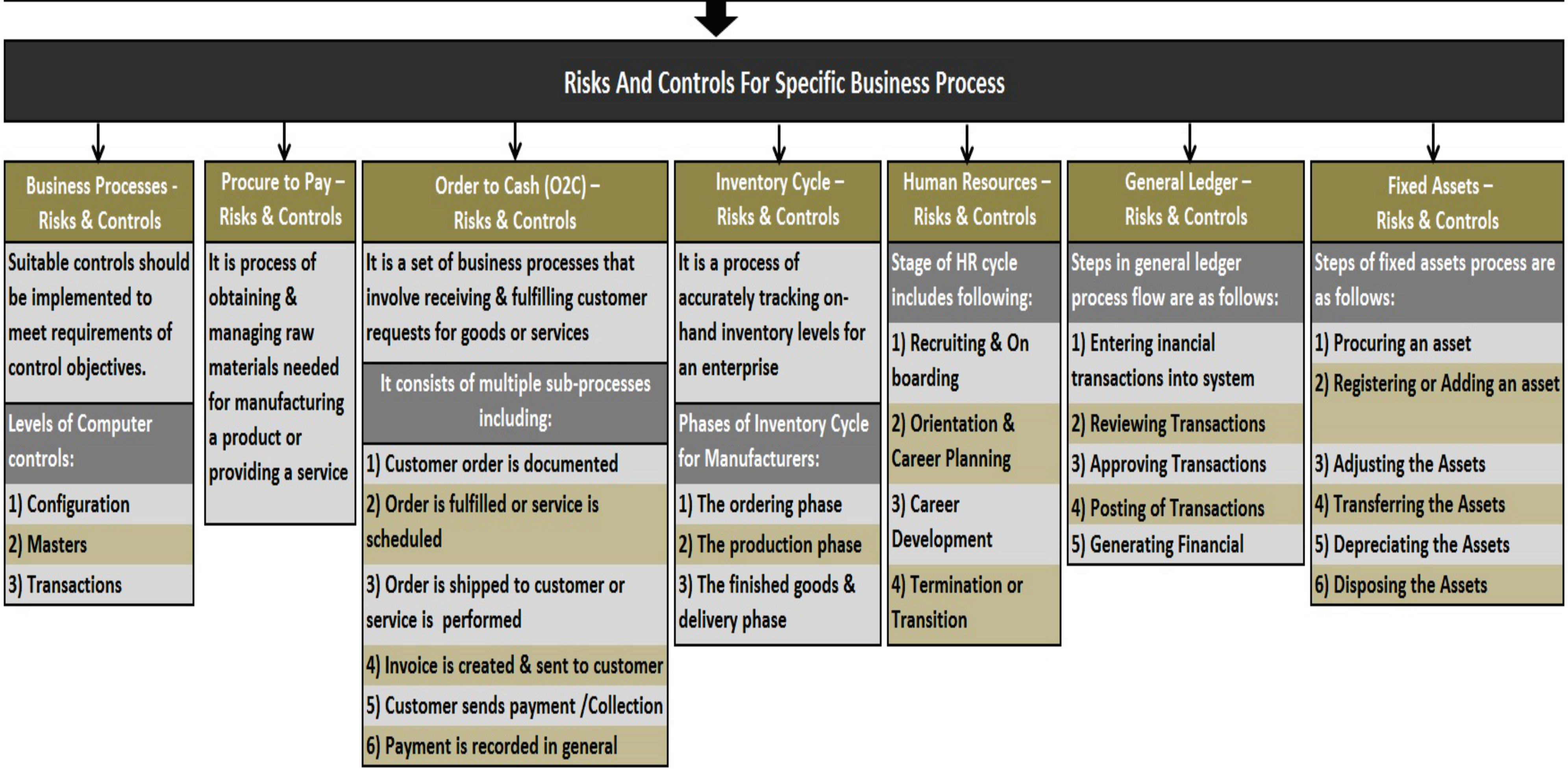
DFD basically provides an overview of:

1) What data a system processes
2) What transformations are performed
3) What data are stored
4) What results are produced and where they flow

Diagrammatic Representation of

1) Customer Order Fulfilment
2) Order to Cash
i) Sales & Marketing
ii) Order Fulfilment
iii) Manufacturing
iv) Receivables
3) Procure to Pay
i) User Department
ii) Procurement Department
iii) Vendor
iv) Stores
v) Accounts Payable

AUTOMATED BUSINESS PROCESS (Chart 1.39)



Risks And Controls For Specific Business Process

Business Processes - Risks & Controls

Suitable controls should be implemented to meet requirements of control objectives.

Levels of Computer controls:

1) Configuration
2) Masters
3) Transactions

Procure to Pay – Risks & Controls

It is process of obtaining & managing raw materials needed for manufacturing a product or providing a service

Order to Cash (O2C) – Risks & Controls

It is a set of business processes that involve receiving & fulfilling customer requests for goods or services

It consists of multiple sub-processes including:

1) Customer order is documented
2) Order is fulfilled or service is scheduled
3) Order is shipped to customer or service is performed
4) Invoice is created & sent to customer
5) Customer sends payment /Collection
6) Payment is recorded in general

Inventory Cycle – Risks & Controls

It is a process of accurately tracking on-hand inventory levels for an enterprise

Phases of Inventory Cycle for Manufacturers:

1) The ordering phase
2) The production phase
3) The finished goods & delivery phase

Human Resources – Risks & Controls

Stage of HR cycle includes following:

1) Recruiting & On boarding
2) Orientation & Career Planning
3) Career Development
4) Termination or Transition

General Ledger – Risks & Controls

Steps in general ledger process flow are as follows:

1) Entering inancial transactions into system
2) Reviewing Transactions
3) Approving Transactions
4) Posting of Transactions
5) Generating Financial

Fixed Assets – Risks & Controls

Steps of fixed assets process are as follows:

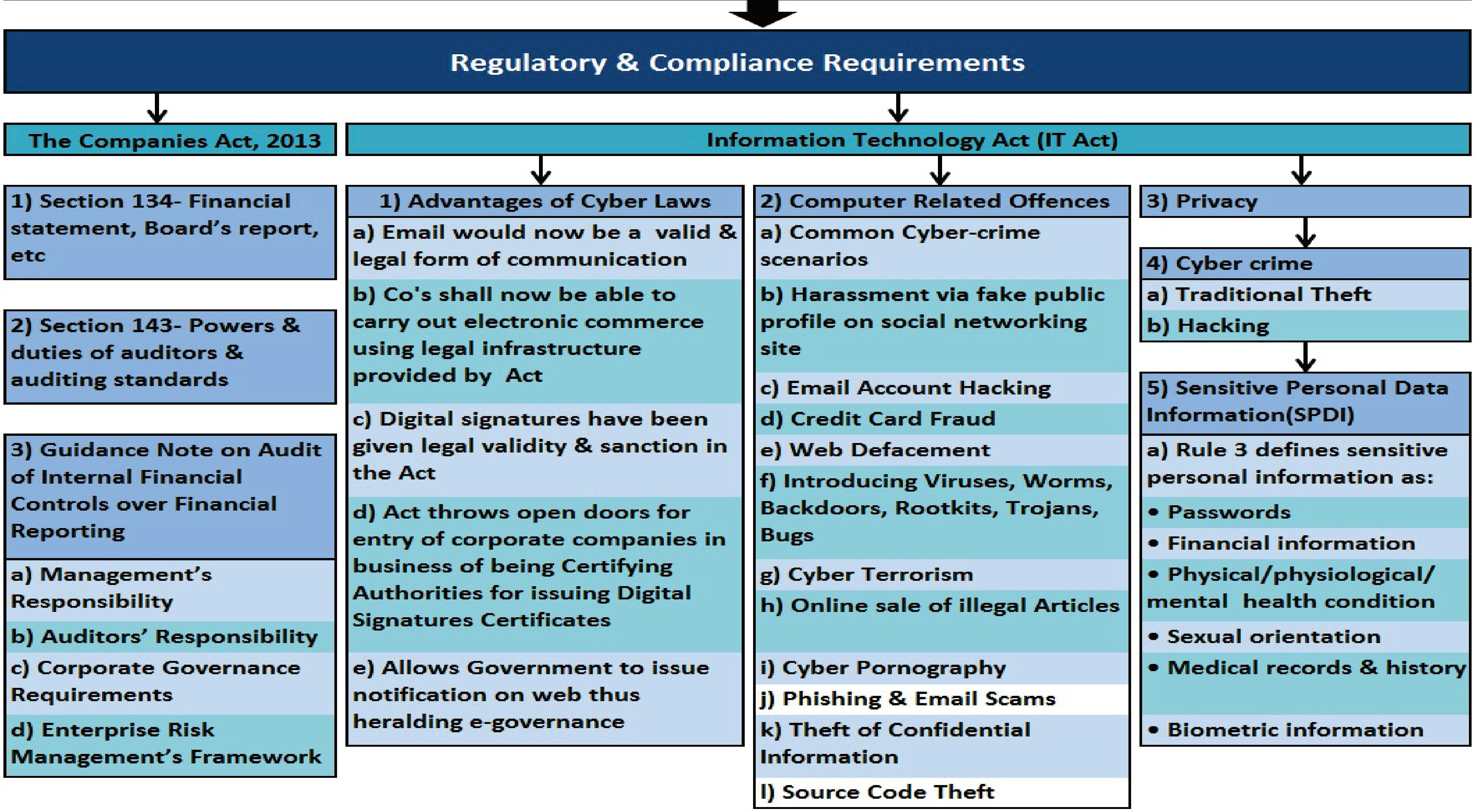
1) Procuring an asset
2) Registering or Adding an asset
3) Adjusting the Assets
4) Transferring the Assets
5) Depreciating the Assets
6) Disposing the Assets

SP CLASSES
For CA -CPT, IPCC & FINAL
Since 2010
your Success Point

Designed By: Swapnil Patni
- CA, CS, LLB, B.Com., CISA
- Expertise knowledge in ISCA, IT, SM, LAW
- Presence all over India at the age of 29
- Also known as the "Motivational Guru"

Team SPC

AUTOMATED BUSINESS PROCESS (Chart 1.40)



Regulatory & Compliance Requirements

The Companies Act, 2013

1) Section 134- Financial statement, Board's report, etc

2) Section 143- Powers & duties of auditors & auditing standards

3) Guidance Note on Audit of Internal Financial Controls over Financial Reporting

a) Management's Responsibility

b) Auditors' Responsibility

c) Corporate Governance Requirements

d) Enterprise Risk Management's Framework

Information Technology Act (IT Act)

1) Advantages of Cyber Laws

a) Email would now be a valid & legal form of communication

b) Co's shall now be able to carry out electronic commerce using legal infrastructure provided by Act

c) Digital signatures have been given legal validity & sanction in the Act

d) Act throws open doors for entry of corporate companies in business of being Certifying Authorities for issuing Digital Signatures Certificates

e) Allows Government to issue notification on web thus heralding e-governance

2) Computer Related Offences

a) Common Cyber-crime scenarios

b) Harassment via fake public profile on social networking site

c) Email Account Hacking

d) Credit Card Fraud

e) Web Defacement

f) Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs

g) Cyber Terrorism

h) Online sale of illegal Articles

i) Cyber Pornography

j) Phishing & Email Scams

k) Theft of Confidential Information

l) Source Code Theft

3) Privacy

4) Cyber crime

a) Traditional Theft

b) Hacking

5) Sensitive Personal Data Information(SPDI)

a) Rule 3 defines sensitive personal information as:

- Passwords
- Financial information
- Physical/physiological/ mental health condition
- Sexual orientation
- Medical records & history
- Biometric information

SP CLASSES

For CA -CPT, IPCC & FINAL

Since 2010

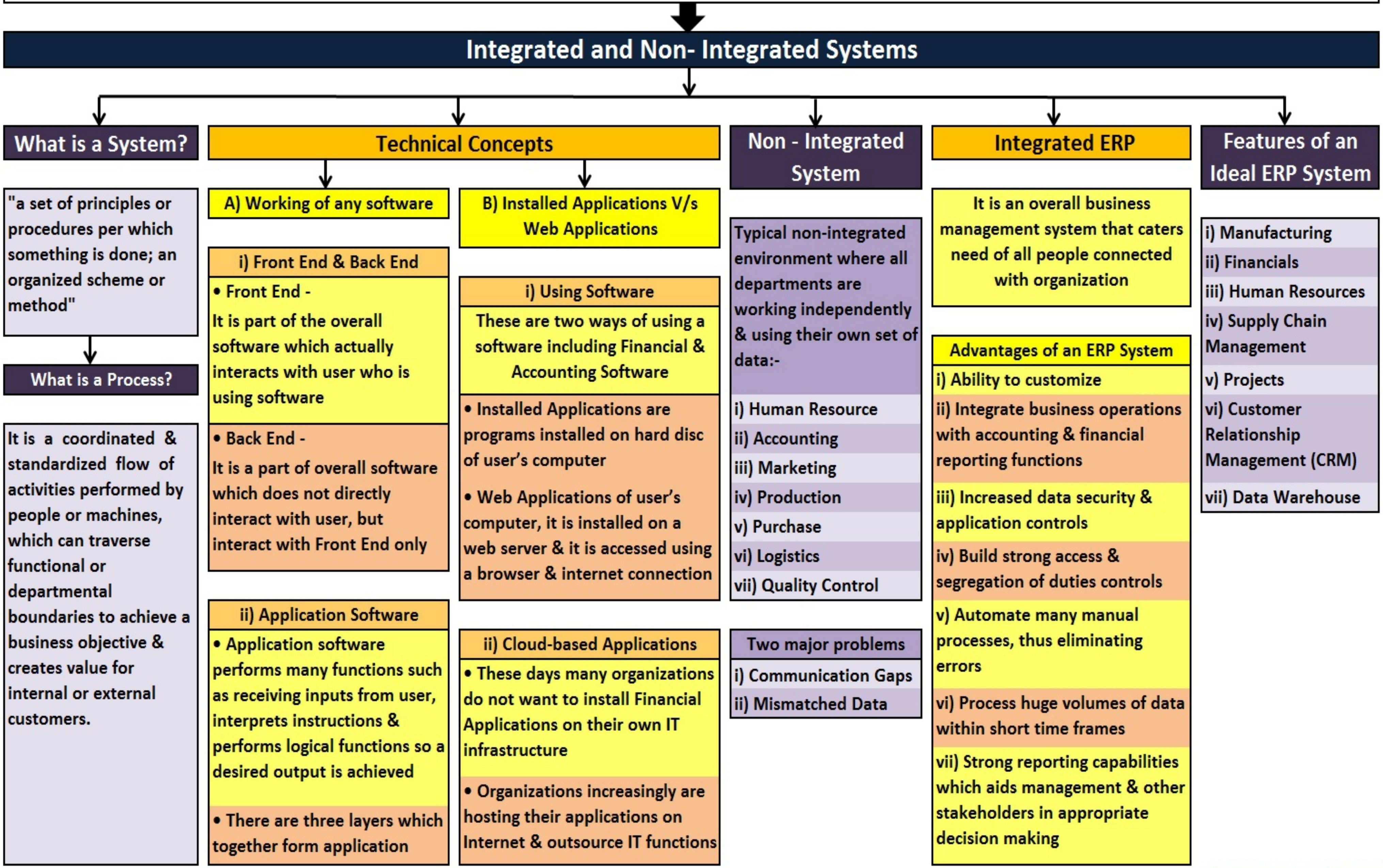
your Success Point

Designed By: **Swapnil Patni**

- CA, CS, LLB, B.Com., CISA
- Expertise knowledge in ISCA, IT, SM, LAW
- Presence all over India at the age of 29
- Also known as the "Motivational Guru"

Team SPC

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.39)



Integrated and Non- Integrated Systems

What is a System?

"a set of principles or procedures per which something is done; an organized scheme or method"

What is a Process?

It is a coordinated & standardized flow of activities performed by people or machines, which can traverse functional or departmental boundaries to achieve a business objective & creates value for internal or external customers.

Technical Concepts

A) Working of any software

i) Front End & Back End

- Front End -

It is part of the overall software which actually interacts with user who is using software

- Back End -

It is a part of overall software which does not directly interact with user, but interact with Front End only

ii) Application Software

- Application software performs many functions such as receiving inputs from user, interprets instructions & performs logical functions so a desired output is achieved
- There are three layers which together form application

B) Installed Applications V/s Web Applications

i) Using Software

These are two ways of using a software including Financial & Accounting Software

- Installed Applications are programs installed on hard disc of user's computer
- Web Applications of user's computer, it is installed on a web server & it is accessed using a browser & internet connection

ii) Cloud-based Applications

- These days many organizations do not want to install Financial Applications on their own IT infrastructure
- Organizations increasingly are hosting their applications on Internet & outsource IT functions

Non - Integrated System

Typical non-integrated environment where all departments are working independently & using their own set of data:-

i) Human Resource
ii) Accounting
iii) Marketing
iv) Production
v) Purchase
vi) Logistics
vii) Quality Control

Two major problems

i) Communication Gaps
ii) Mismatched Data

Integrated ERP

It is an overall business management system that caters need of all people connected with organization

Advantages of an ERP System

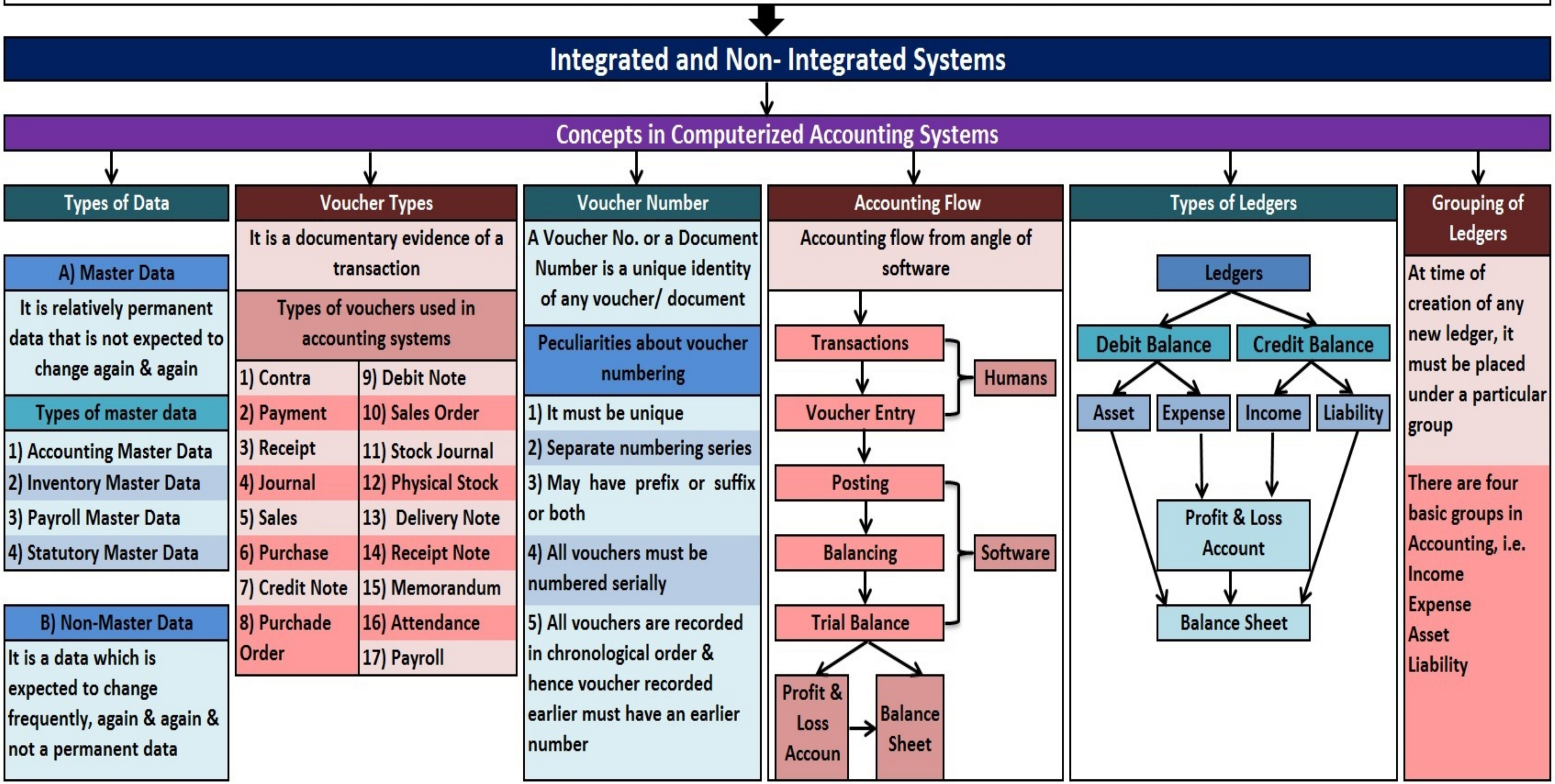
i) Ability to customize
ii) Integrate business operations with accounting & financial reporting functions
iii) Increased data security & application controls
iv) Build strong access & segregation of duties controls
v) Automate many manual processes, thus eliminating errors
vi) Process huge volumes of data within short time frames
vii) Strong reporting capabilities which aids management & other stakeholders in appropriate decision making

Features of an Ideal ERP System

i) Manufacturing
ii) Financials
iii) Human Resources
iv) Supply Chain Management
v) Projects
vi) Customer Relationship Management (CRM)
vii) Data Warehouse

(Continue on Chart 2.40)

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.40)



Integrated and Non- Integrated Systems

Concepts in Computerized Accounting Systems

Types of Data

A) Master Data

It is relatively permanent data that is not expected to change again & again

Types of master data

1) Accounting Master Data
2) Inventory Master Data
3) Payroll Master Data
4) Statutory Master Data

B) Non-Master Data

It is a data which is expected to change frequently, again & again & not a permanent data

Voucher Types

It is a documentary evidence of a transaction

Types of vouchers used in accounting systems

1) Contra	9) Debit Note
2) Payment	10) Sales Order
3) Receipt	11) Stock Journal
4) Journal	12) Physical Stock
5) Sales	13) Delivery Note
6) Purchase	14) Receipt Note
7) Credit Note	15) Memorandum
8) Purchade Order	16) Attendance
	17) Payroll

Voucher Number

A Voucher No. or a Document Number is a unique identity of any voucher/ document

Peculiarities about voucher numbering

1) It must be unique
2) Separate numbering series
3) May have prefix or suffix or both
4) All vouchers must be numbered serially
5) All vouchers are recorded in chronological order & hence voucher recorded earlier must have an earlier number

Accounting Flow

Accounting flow from angle of software

Types of Ledgers

Grouping of Ledgers

At time of creation of any new ledger, it must be placed under a particular group

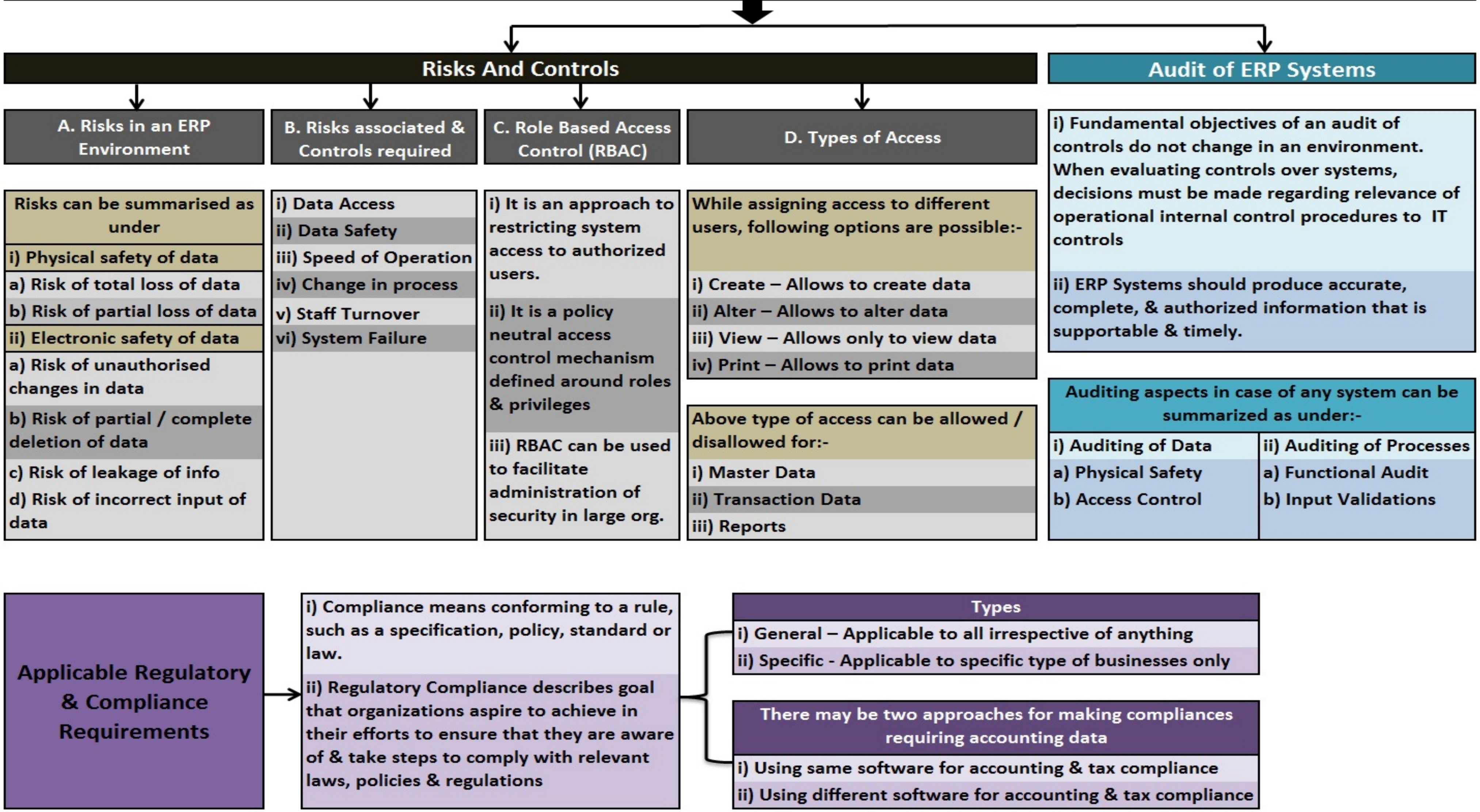
There are four basic groups in Accounting, i.e.
Income
Expense
Asset
Liability

SP CLASSES
For CA -CPT, IPCC & FINAL
Since 2010
your Success Point

Designed By: **Swapnil Patni**
- CA, CS, LLB, B.Com., CISA
- Expertise knowledge in ISCA, IT, SM, LAW
- Presence all over India at the age of 29
- Also known as the "Motivational Guru"

Team SPC

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.41)



Risks And Controls

A. Risks in an ERP Environment

Risks can be summarised as under

- i) Physical safety of data
  - a) Risk of total loss of data
  - b) Risk of partial loss of data
- ii) Electronic safety of data
  - a) Risk of unauthorised changes in data
  - b) Risk of partial / complete deletion of data
  - c) Risk of leakage of info
  - d) Risk of incorrect input of data

B. Risks associated & Controls required

- i) Data Access
- ii) Data Safety
- iii) Speed of Operation
- iv) Change in process
- v) Staff Turnover
- vi) System Failure

C. Role Based Access Control (RBAC)

i) It is an approach to restricting system access to authorized users.

ii) It is a policy neutral access control mechanism defined around roles & privileges

iii) RBAC can be used to facilitate administration of security in large org.

D. Types of Access

While assigning access to different users, following options are possible:-

- i) Create – Allows to create data
- ii) Alter – Allows to alter data
- iii) View – Allows only to view data
- iv) Print – Allows to print data

Above type of access can be allowed / disallowed for:-

- i) Master Data
- ii) Transaction Data
- iii) Reports

Audit of ERP Systems

i) Fundamental objectives of an audit of controls do not change in an environment. When evaluating controls over systems, decisions must be made regarding relevance of operational internal control procedures to IT controls

ii) ERP Systems should produce accurate, complete, & authorized information that is supportable & timely.

Auditing aspects in case of any system can be summarized as under:-

i) Auditing of Data	ii) Auditing of Processes
a) Physical Safety	a) Functional Audit
b) Access Control	b) Input Validations

Applicable Regulatory & Compliance Requirements

i) Compliance means conforming to a rule, such as a specification, policy, standard or law.

ii) Regulatory Compliance describes goal that organizations aspire to achieve in their efforts to ensure that they are aware of & take steps to comply with relevant laws, policies & regulations

Types

- i) General – Applicable to all irrespective of anything
- ii) Specific - Applicable to specific type of businesses only

There may be two approaches for making compliances requiring accounting data

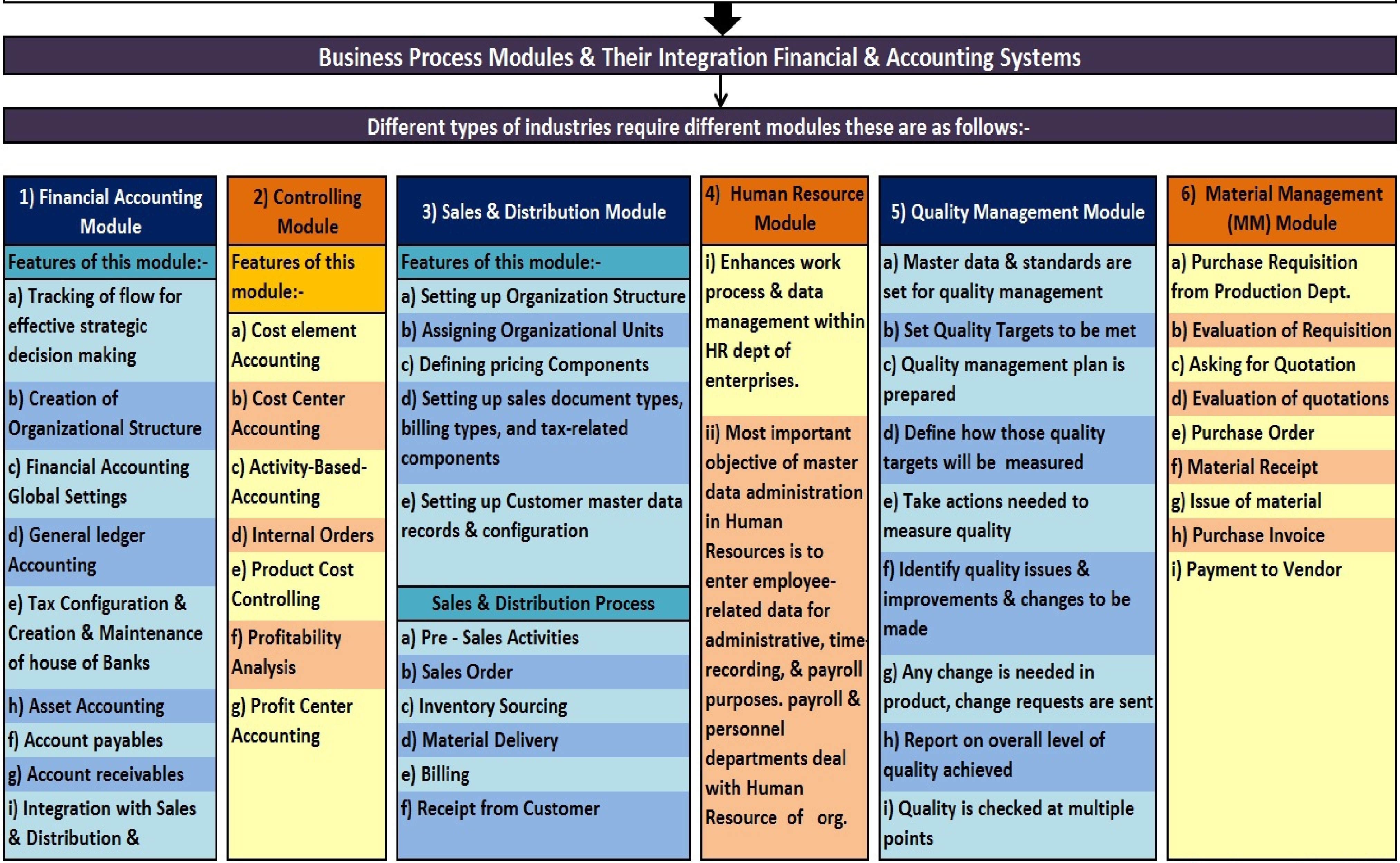
- i) Using same software for accounting & tax compliance
- ii) Using different software for accounting & tax compliance

SP CLASSES
For CA -CPT, IPCC & FINAL
Since 2010
your Success Point

Designed By: Swapnil Patni
- CA, CS, LLB, B.Com., CISA
- Expertise knowledge in ISCA, IT, SM, LAW
- Presence all over India at the age of 29
- Also known as the "Motivational Guru"

Team SPC

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.42)



Business Process Modules & Their Integration Financial & Accounting Systems

Different types of industries require different modules these are as follows:-

1) Financial Accounting Module

Features of this module:-

a) Tracking of flow for effective strategic decision making

b) Creation of Organizational Structure

c) Financial Accounting Global Settings

d) General ledger Accounting

e) Tax Configuration & Creation & Maintenance of house of Banks

h) Asset Accounting

f) Account payables

g) Account receivables

i) Integration with Sales & Distribution &

2) Controlling Module

Features of this module:-

a) Cost element Accounting

b) Cost Center Accounting

c) Activity-Based-Accounting

d) Internal Orders

e) Product Cost Controlling

f) Profitability Analysis

g) Profit Center Accounting

3) Sales & Distribution Module

Features of this module:-

a) Setting up Organization Structure

b) Assigning Organizational Units

c) Defining pricing Components

d) Setting up sales document types, billing types, and tax-related components

e) Setting up Customer master data records & configuration

Sales & Distribution Process

a) Pre - Sales Activities

b) Sales Order

c) Inventory Sourcing

d) Material Delivery

e) Billing

f) Receipt from Customer

4) Human Resource Module

i) Enhances work process & data management within HR dept of enterprises.

ii) Most important objective of master data administration in Human Resources is to enter employee-related data for administrative, time-recording, & payroll purposes. payroll & personnel departments deal with Human Resource of org.

5) Quality Management Module

a) Master data & standards are set for quality management

b) Set Quality Targets to be met

c) Quality management plan is prepared

d) Define how those quality targets will be measured

e) Take actions needed to measure quality

f) Identify quality issues & improvements & changes to be made

g) Any change is needed in product, change requests are sent

h) Report on overall level of quality achieved

i) Quality is checked at multiple points

6) Material Management (MM) Module

a) Purchase Requisition from Production Dept.

b) Evaluation of Requisition

c) Asking for Quotation

d) Evaluation of quotations

e) Purchase Order

f) Material Receipt

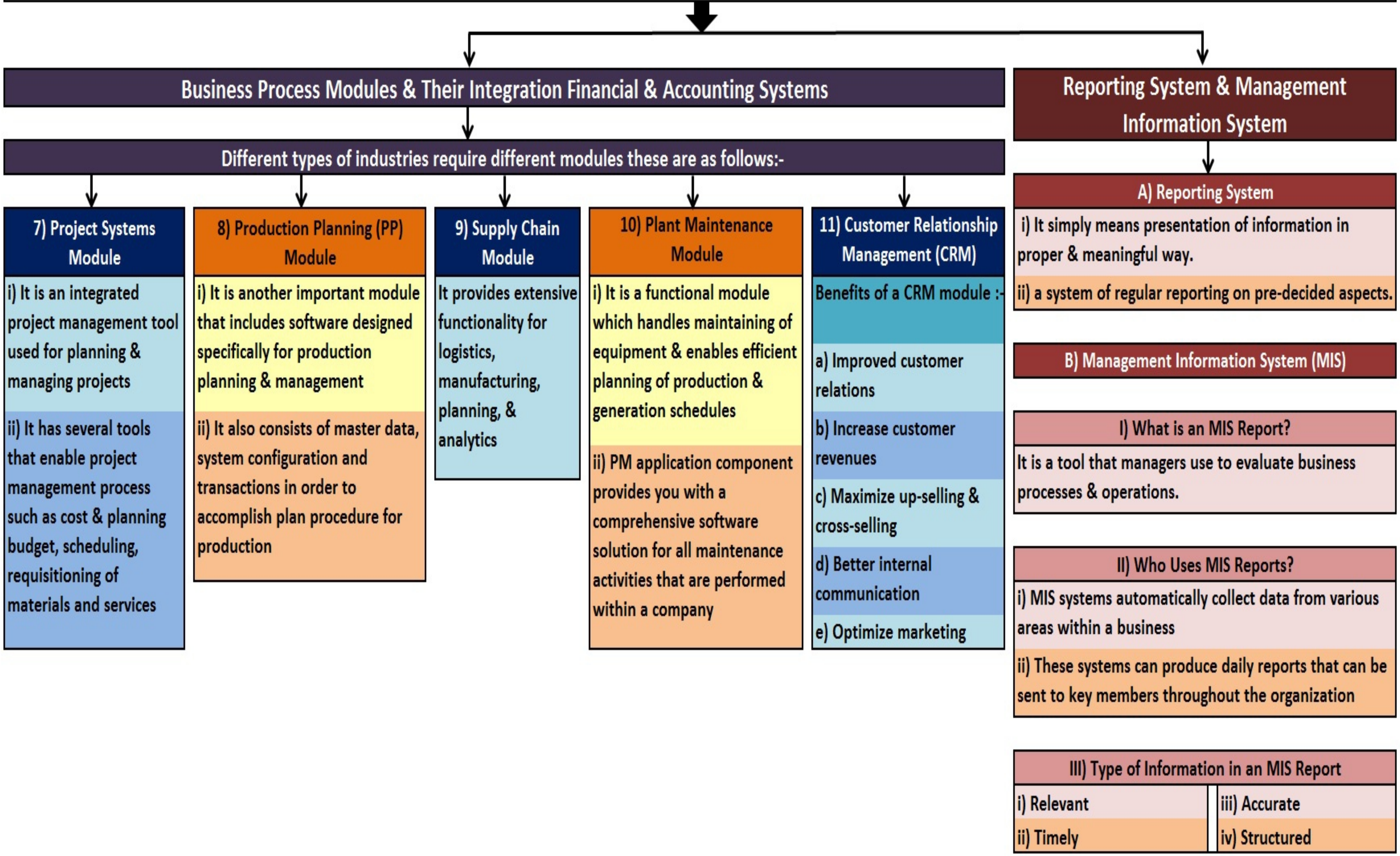
g) Issue of material

h) Purchase Invoice

i) Payment to Vendor

(Continue on Chart 2.43)

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.43)



Business Process Modules & Their Integration Financial & Accounting Systems

Different types of industries require different modules these are as follows:-

7) Project Systems Module

i) It is an integrated project management tool used for planning & managing projects

ii) It has several tools that enable project management process such as cost & planning budget, scheduling, requisitioning of materials and services

8) Production Planning (PP) Module

i) It is another important module that includes software designed specifically for production planning & management

ii) It also consists of master data, system configuration and transactions in order to accomplish plan procedure for production

9) Supply Chain Module

It provides extensive functionality for logistics, manufacturing, planning, & analytics

10) Plant Maintenance Module

i) It is a functional module which handles maintaining of equipment & enables efficient planning of production & generation schedules

ii) PM application component provides you with a comprehensive software solution for all maintenance activities that are performed within a company

11) Customer Relationship Management (CRM)

Benefits of a CRM module :-

a) Improved customer relations

b) Increase customer revenues

c) Maximize up-selling & cross-selling

d) Better internal communication

e) Optimize marketing

Reporting System & Management Information System

A) Reporting System

i) It simply means presentation of information in proper & meaningful way.

ii) a system of regular reporting on pre-decided aspects.

B) Management Information System (MIS)

I) What is an MIS Report?

It is a tool that managers use to evaluate business processes & operations.

II) Who Uses MIS Reports?

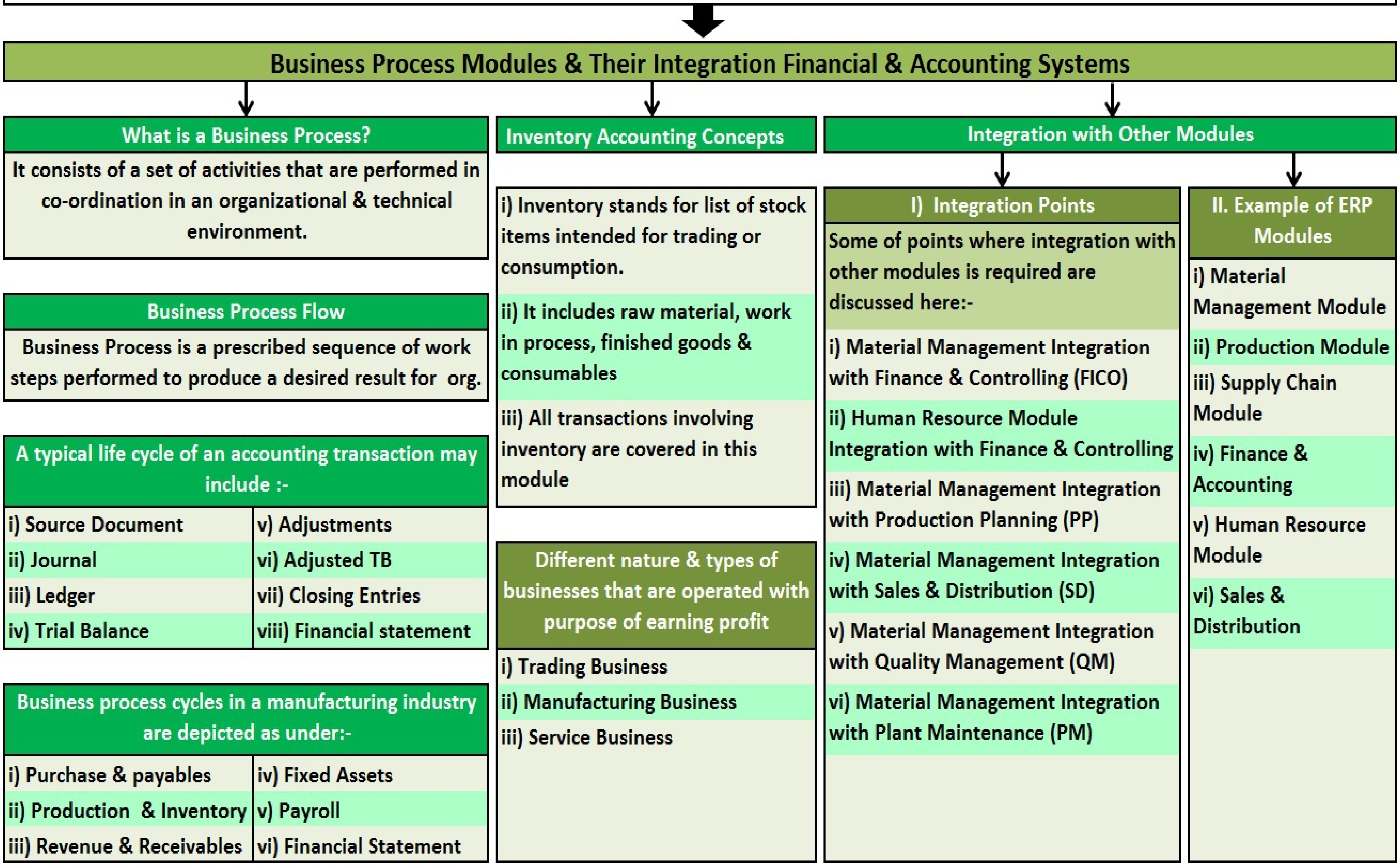
i) MIS systems automatically collect data from various areas within a business

ii) These systems can produce daily reports that can be sent to key members throughout the organization

III) Type of Information in an MIS Report

i) Relevant	iii) Accurate
ii) Timely	iv) Structured

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.44)



Business Process Modules & Their Integration Financial & Accounting Systems

What is a Business Process?

It consists of a set of activities that are performed in co-ordination in an organizational & technical environment.

Business Process Flow

Business Process is a prescribed sequence of work steps performed to produce a desired result for org.

A typical life cycle of an accounting transaction may include :-

i) Source Document
ii) Journal
iii) Ledger
iv) Trial Balance
v) Adjustments
vi) Adjusted TB
vii) Closing Entries
viii) Financial statement

Business process cycles in a manufacturing industry are depicted as under:-

i) Purchase & payables
ii) Production & Inventory
iii) Revenue & Receivables
iv) Fixed Assets
v) Payroll
vi) Financial Statement

Inventory Accounting Concepts

i) Inventory stands for list of stock items intended for trading or consumption.

ii) It includes raw material, work in process, finished goods & consumables

iii) All transactions involving inventory are covered in this module

Different nature & types of businesses that are operated with purpose of earning profit

i) Trading Business
ii) Manufacturing Business
iii) Service Business

Integration with Other Modules

I) Integration Points

Some of points where integration with other modules is required are discussed here:-

i) Material Management Integration with Finance & Controlling (FICO)

ii) Human Resource Module Integration with Finance & Controlling

iii) Material Management Integration with Production Planning (PP)

iv) Material Management Integration with Sales & Distribution (SD)

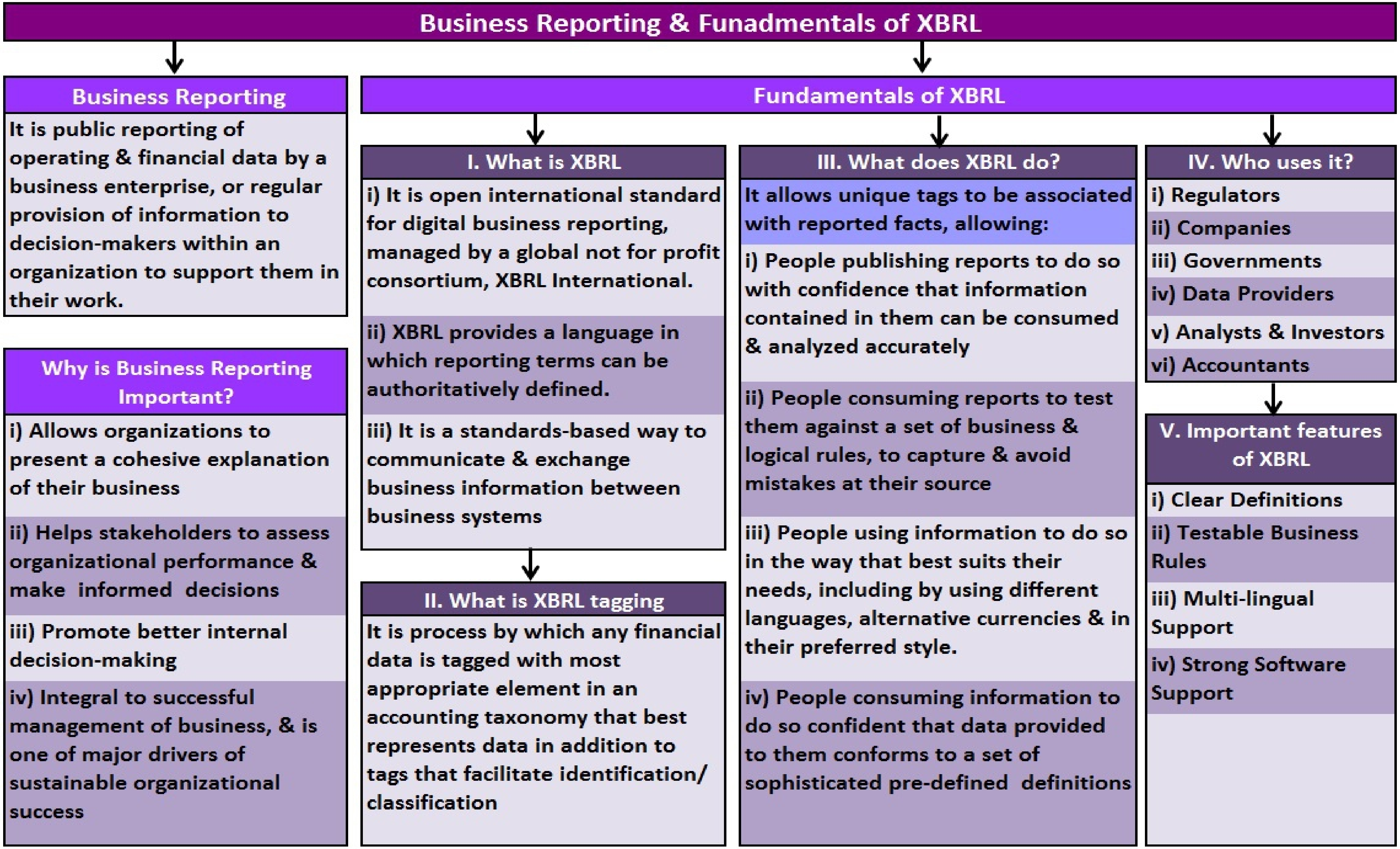
v) Material Management Integration with Quality Management (QM)

vi) Material Management Integration with Plant Maintenance (PM)

II. Example of ERP Modules

i) Material Management Module
ii) Production Module
iii) Supply Chain Module
iv) Finance & Accounting
v) Human Resource Module
vi) Sales & Distribution

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.45)



Business Reporting & Funadmentals of XBRL

Business Reporting

It is public reporting of operating & financial data by a business enterprise, or regular provision of information to decision-makers within an organization to support them in their work.

Why is Business Reporting Important?

i) Allows organizations to present a cohesive explanation of their business

ii) Helps stakeholders to assess organizational performance & make informed decisions

iii) Promote better internal decision-making

iv) Integral to successful management of business, & is one of major drivers of sustainable organizational success

Fundamentals of XBRL

I. What is XBRL

i) It is open international standard for digital business reporting, managed by a global not for profit consortium, XBRL International.

ii) XBRL provides a language in which reporting terms can be authoritatively defined.

iii) It is a standards-based way to communicate & exchange business information between business systems

II. What is XBRL tagging

It is process by which any financial data is tagged with most appropriate element in an accounting taxonomy that best represents data in addition to tags that facilitate identification/ classification

III. What does XBRL do?

It allows unique tags to be associated with reported facts, allowing:

i) People publishing reports to do so with confidence that information contained in them can be consumed & analyzed accurately

ii) People consuming reports to test them against a set of business & logical rules, to capture & avoid mistakes at their source

iii) People using information to do so in the way that best suits their needs, including by using different languages, alternative currencies & in their preferred style.

iv) People consuming information to do so confident that data provided to them conforms to a set of sophisticated pre-defined definitions

IV. Who uses it?

i) Regulators

ii) Companies

iii) Governments

iv) Data Providers

v) Analysts & Investors

vi) Accountants

V. Important features of XBRL

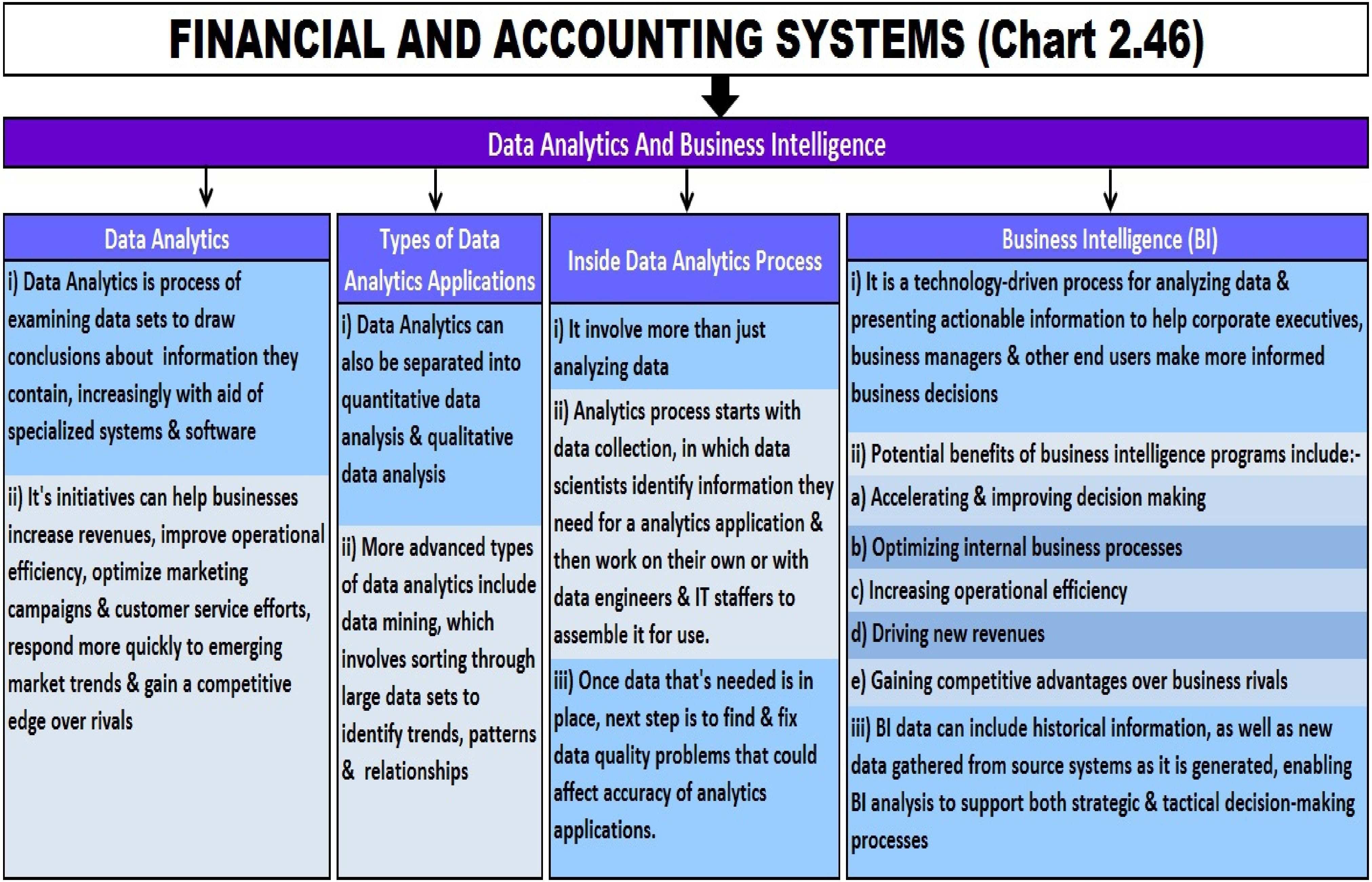
i) Clear Definitions

ii) Testable Business Rules

iii) Multi-lingual Support

iv) Strong Software Support

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.46)



Data Analytics And Business Intelligence

Data Analytics

i) Data Analytics is process of examining data sets to draw conclusions about information they contain, increasingly with aid of specialized systems & software

ii) It's initiatives can help businesses increase revenues, improve operational efficiency, optimize marketing campaigns & customer service efforts, respond more quickly to emerging market trends & gain a competitive edge over rivals

Types of Data Analytics Applications

i) Data Analytics can also be separated into quantitative data analysis & qualitative data analysis

ii) More advanced types of data analytics include data mining, which involves sorting through large data sets to identify trends, patterns & relationships

Inside Data Analytics Process

i) It involve more than just analyzing data

ii) Analytics process starts with data collection, in which data scientists identify information they need for a analytics application & then work on their own or with data engineers & IT staffers to assemble it for use.

iii) Once data that's needed is in place, next step is to find & fix data quality problems that could affect accuracy of analytics applications.

Business Intelligence (BI)

i) It is a technology-driven process for analyzing data & presenting actionable information to help corporate executives, business managers & other end users make more informed business decisions

ii) Potential benefits of business intelligence programs include:-

a) Accelerating & improving decision making

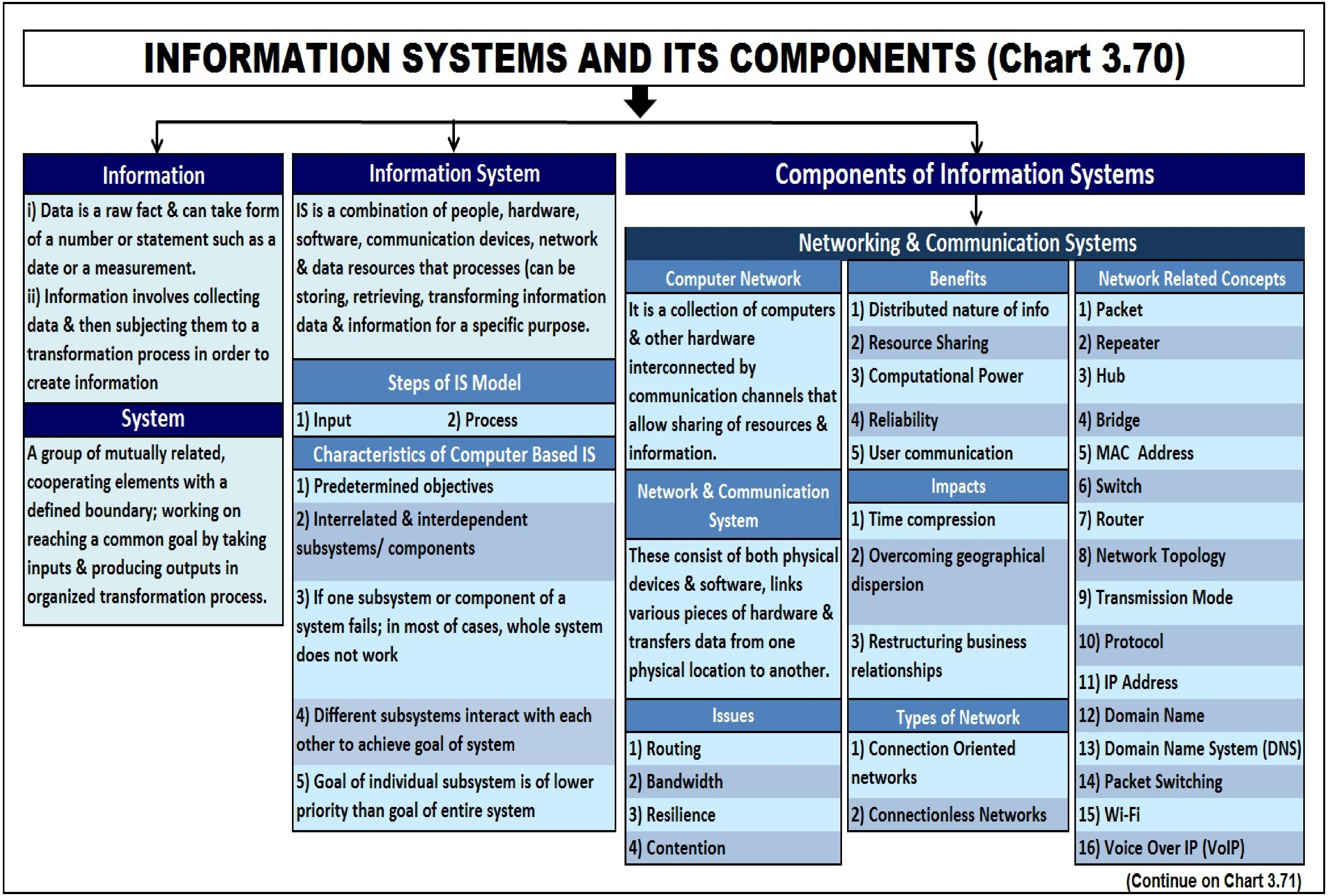
b) Optimizing internal business processes

c) Increasing operational efficiency

d) Driving new revenues

e) Gaining competitive advantages over business rivals

iii) BI data can include historical information, as well as new data gathered from source systems as it is generated, enabling BI analysis to support both strategic & tactical decision-making processes



INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.70)

Information

i) Data is a raw fact & can take form of a number or statement such as a date or a measurement.

ii) Information involves collecting data & then subjecting them to a transformation process in order to create information

System

A group of mutually related, cooperating elements with a defined boundary; working on reaching a common goal by taking inputs & producing outputs in organized transformation process.

Information System

IS is a combination of people, hardware, software, communication devices, network & data resources that processes (can be storing, retrieving, transforming information data & information for a specific purpose.

Steps of IS Model

1) Input
2) Process

Characteristics of Computer Based IS

1) Predetermined objectives
2) Interrelated & interdependent subsystems/ components
3) If one subsystem or component of a system fails; in most of cases, whole system does not work
4) Different subsystems interact with each other to achieve goal of system
5) Goal of individual subsystem is of lower priority than goal of entire system

Components of Information Systems

Networking & Communication Systems

Computer Network

It is a collection of computers & other hardware interconnected by communication channels that allow sharing of resources & information.

Network & Communication System

These consist of both physical devices & software, links various pieces of hardware & transfers data from one physical location to another.

Issues

1) Routing
2) Bandwidth
3) Resilience
4) Contention

Benefits

1) Distributed nature of info
2) Resource Sharing
3) Computational Power
4) Reliability
5) User communication

Impacts

1) Time compression
2) Overcoming geographical dispersion
3) Restructuring business relationships

Types of Network

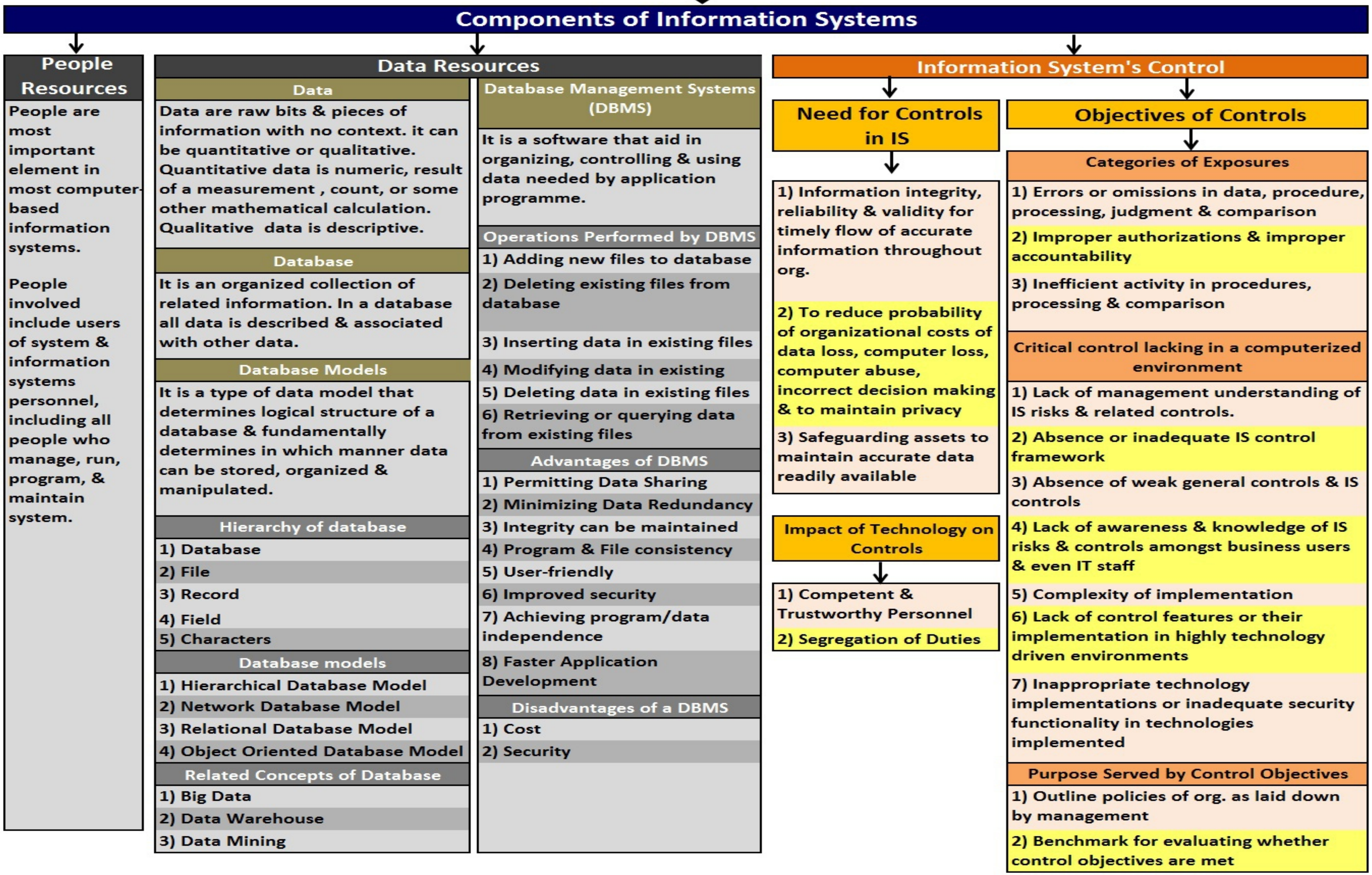
1) Connection Oriented networks
2) Connectionless Networks

Network Related Concepts

1) Packet
2) Repeater
3) Hub
4) Bridge
5) MAC Address
6) Switch
7) Router
8) Network Topology
9) Transmission Mode
10) Protocol
11) IP Address
12) Domain Name
13) Domain Name System (DNS)
14) Packet Switching
15) Wi-Fi
16) Voice Over IP (VoIP)

(Continue on Chart 3.71)

INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.71)



Components of Information Systems

People Resources

People are most important element in most computer-based information systems.

People involved include users of system & information systems personnel, including all people who manage, run, program, & maintain system.

Data Resources

Data

Data are raw bits & pieces of information with no context. it can be quantitative or qualitative. Quantitative data is numeric, result of a measurement , count, or some other mathematical calculation. Qualitative data is descriptive.

Database

It is an organized collection of related information. In a database all data is described & associated with other data.

Database Models

It is a type of data model that determines logical structure of a database & fundamentally determines in which manner data can be stored, organized & manipulated.

Hierarchy of database

1) Database
2) File
3) Record
4) Field
5) Characters

Database models

1) Hierarchical Database Model
2) Network Database Model
3) Relational Database Model
4) Object Oriented Database Model

Related Concepts of Database

1) Big Data
2) Data Warehouse
3) Data Mining

Database Management Systems (DBMS)

It is a software that aid in organizing, controlling & using data needed by application programme.

Operations Performed by DBMS

1) Adding new files to database
2) Deleting existing files from database
3) Inserting data in existing files
4) Modifying data in existing
5) Deleting data in existing files
6) Retrieving or querying data from existing files

Advantages of DBMS

1) Permitting Data Sharing
2) Minimizing Data Redundancy
3) Integrity can be maintained
4) Program & File consistency
5) User-friendly
6) Improved security
7) Achieving program/data independence
8) Faster Application Development

Disadvantages of a DBMS

1) Cost
2) Security

Information System's Control

Need for Controls in IS

1) Information integrity, reliability & validity for timely flow of accurate information throughout org.

2) To reduce probability of organizational costs of data loss, computer loss, computer abuse, incorrect decision making & to maintain privacy

3) Safeguarding assets to maintain accurate data readily available

Impact of Technology on Controls

1) Competent & Trustworthy Personnel
2) Segregation of Duties

Objectives of Controls

Categories of Exposures

1) Errors or omissions in data, procedure, processing, judgment & comparison
2) Improper authorizations & improper accountability
3) Inefficient activity in procedures, processing & comparison

Critical control lacking in a computerized environment

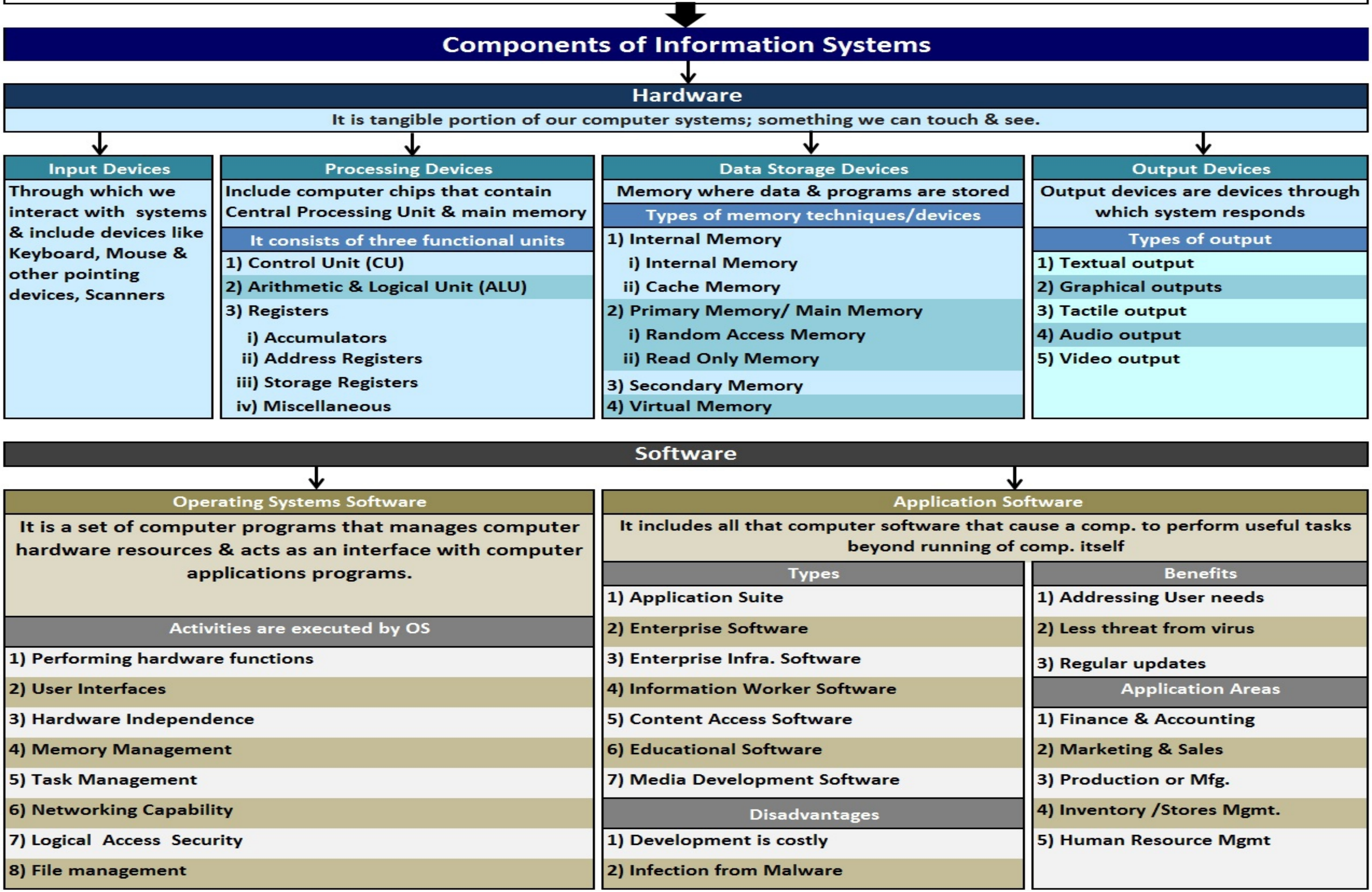
1) Lack of management understanding of IS risks & related controls.
2) Absence or inadequate IS control framework
3) Absence of weak general controls & IS controls
4) Lack of awareness & knowledge of IS risks & controls amongst business users & even IT staff
5) Complexity of implementation
6) Lack of control features or their implementation in highly technology driven environments
7) Inappropriate technology implementations or inadequate security functionality in technologies implemented

Purpose Served by Control Objectives

1) Outline policies of org. as laid down by management
2) Benchmark for evaluating whether control objectives are met

(Continue on Chart 3.72)

INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.72)



Components of Information Systems

Hardware

It is tangible portion of our computer systems; something we can touch & see.

Input Devices

Through which we interact with systems & include devices like Keyboard, Mouse & other pointing devices, Scanners

Processing Devices

Include computer chips that contain Central Processing Unit & main memory

It consists of three functional units

1) Control Unit (CU)
2) Arithmetic & Logical Unit (ALU)
3) Registers
   - i) Accumulators
   - ii) Address Registers
   - iii) Storage Registers
   - iv) Miscellaneous

Data Storage Devices

Memory where data & programs are stored

Types of memory techniques/devices

1) Internal Memory
   - i) Internal Memory
   - ii) Cache Memory
2) Primary Memory/ Main Memory
   - i) Random Access Memory
   - ii) Read Only Memory
3) Secondary Memory
4) Virtual Memory

Output Devices

Output devices are devices through which system responds

Types of output

1) Textual output
2) Graphical outputs
3) Tactile output
4) Audio output
5) Video output

Software

Operating Systems Software

It is a set of computer programs that manages computer hardware resources & acts as an interface with computer applications programs.

Activities are executed by OS

1) Performing hardware functions
2) User Interfaces
3) Hardware Independence
4) Memory Management
5) Task Management
6) Networking Capability
7) Logical Access Security
8) File management

Application Software

It includes all that computer software that cause a comp. to perform useful tasks beyond running of comp. itself

Types

1) Application Suite
2) Enterprise Software
3) Enterprise Infra. Software
4) Information Worker Software
5) Content Access Software
6) Educational Software
7) Media Development Software

Disadvantages

1) Development is costly
2) Infection from Malware

Benefits

1) Addressing User needs
2) Less threat from virus
3) Regular updates

Application Areas

1) Finance & Accounting
2) Marketing & Sales
3) Production or Mfg.
4) Inventory /Stores Mgmt.
5) Human Resource Mgmt

INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.73)

Classification of Information System's Controls

Objective of Controls

1) Preventive Controls

These controls prevent errors, omissions, or security incidents from occurring

2) Detective Controls

These controls are designed to detect errors, omissions or malicious acts that occur & report occurrence.

Characteristics

- i) Clear understanding of lawful activities
- ii) Established mechanism to refer reported unlawful activities to appropriate person or group.
- iii) Interaction with preventive control to prevent such acts from occurring
- iv) Surprise checks by supervisor

3) Corrective Controls

It is desirable to correct errors, omissions, or incidents once they have been detected

Characteristics

- i) Minimizing impact of threat.
- ii) Identifying cause of problem
- iii) Providing remedy to problems discovered by detective controls
- iv) Getting feedback from preventive & detective controls.
- v) Correcting error arising from a problem
- vi) Modifying processing systems to minimize future occurrences of incidents.

Nature of Information System Resources

1) Environmental Controls

Controls relating to IT environment

Controls for Environmental Exposures

- 1) Fire Damage
- 2) Power Spikes
- 3) Water Damage
- 4) Pollution Damage & others

2) Physical Access Controls

This includes abuse of data processing resources

Controls for Physical Exposures

- i) Locks on Doors
- ii) Physical Identiication Medium
- iii) Logging on Facilities
- 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

3) Logical Access Controls

These are controls relating to logical access to information resources

Technical Exposures

- 1) Data Diddling
- 2) Bomb
- 3) Christmas Card
- 4) Worm
- 5) Rounding Down
- 6) Salami Techniques
- 7) Trap Doors
- 8) Spooing

Asynchronous Attacks

- 1) Data Leakage
- 2) Subversive Attacks
- 3) Wire tapping
- 4) Piggybacking

Logical Access Violators

- 1) Hackers
- 2) Employees
- 3) IS Personnel
- 4) Former Employees
- 5) 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) Mobile Computing

6) Operating System Access Control

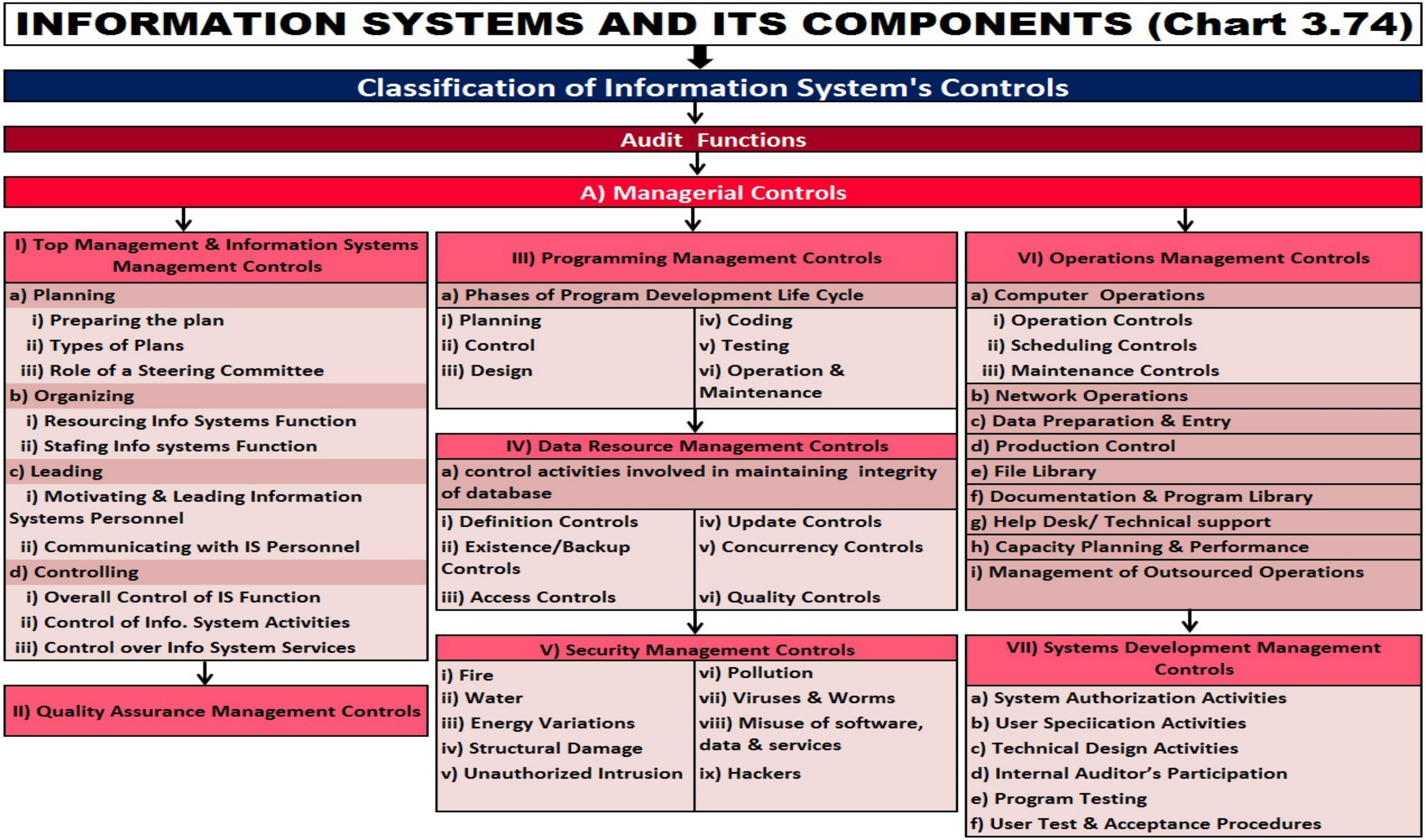
- i) Automated terminal identiication
- ii) Terminal log-in procedures
- iii) Access Token
- iv) Access Control List
- v) Discretionary Access Control
- vi) User identiication & authentication
- vii) Password management system
- viii) Use of system utilities
- ix) Duress alarm to safeguard users
- x)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

(Continue on Chart 3.74)

SP CLASSES
For CA -CPT, IPCC & FINAL
Since 2010
your Success Point

Designed By: Swapnil Patni
- CA, CS, LLB, B.Com., CISA
- Expertise knowledge in ISCA, IT, SM, LAW
- Presence all over India at the age of 29
- Also known as the "Motivational Guru"

Team SPC



INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.74)

Classification of Information System's Controls

Audit Functions

A) Managerial Controls

I) Top Management & Information Systems Management Controls

- a) Planning
  - i) Preparing the plan
  - ii) Types of Plans
  - iii) Role of a Steering Committee
- b) Organizing
  - i) Resourcing Info Systems Function
  - ii) Stafing Info systems Function
- c) Leading
  - i) Motivating & Leading Information Systems Personnel
  - ii) Communicating with IS Personnel
- d) Controlling
  - i) Overall Control of IS Function
  - ii) Control of Info. System Activities
  - iii) Control over Info System Services

II) Quality Assurance Management Controls

III) Programming Management Controls

- a) Phases of Program Development Life Cycle

i) Planning	iv) Coding
ii) Control	v) Testing
iii) Design	vi) Operation & Maintenance

IV) Data Resource Management Controls

- a) control activities involved in maintaining integrity of database

i) Definition Controls	iv) Update Controls
ii) Existence/Backup Controls	v) Concurrency Controls
iii) Access Controls	vi) Quality Controls

V) Security Management Controls

i) Fire	vi) Pollution
ii) Water	vii) Viruses & Worms
iii) Energy Variations	viii) Misuse of software, data & services
iv) Structural Damage	ix) Hackers
v) Unauthorized Intrusion	

VI) Operations Management Controls

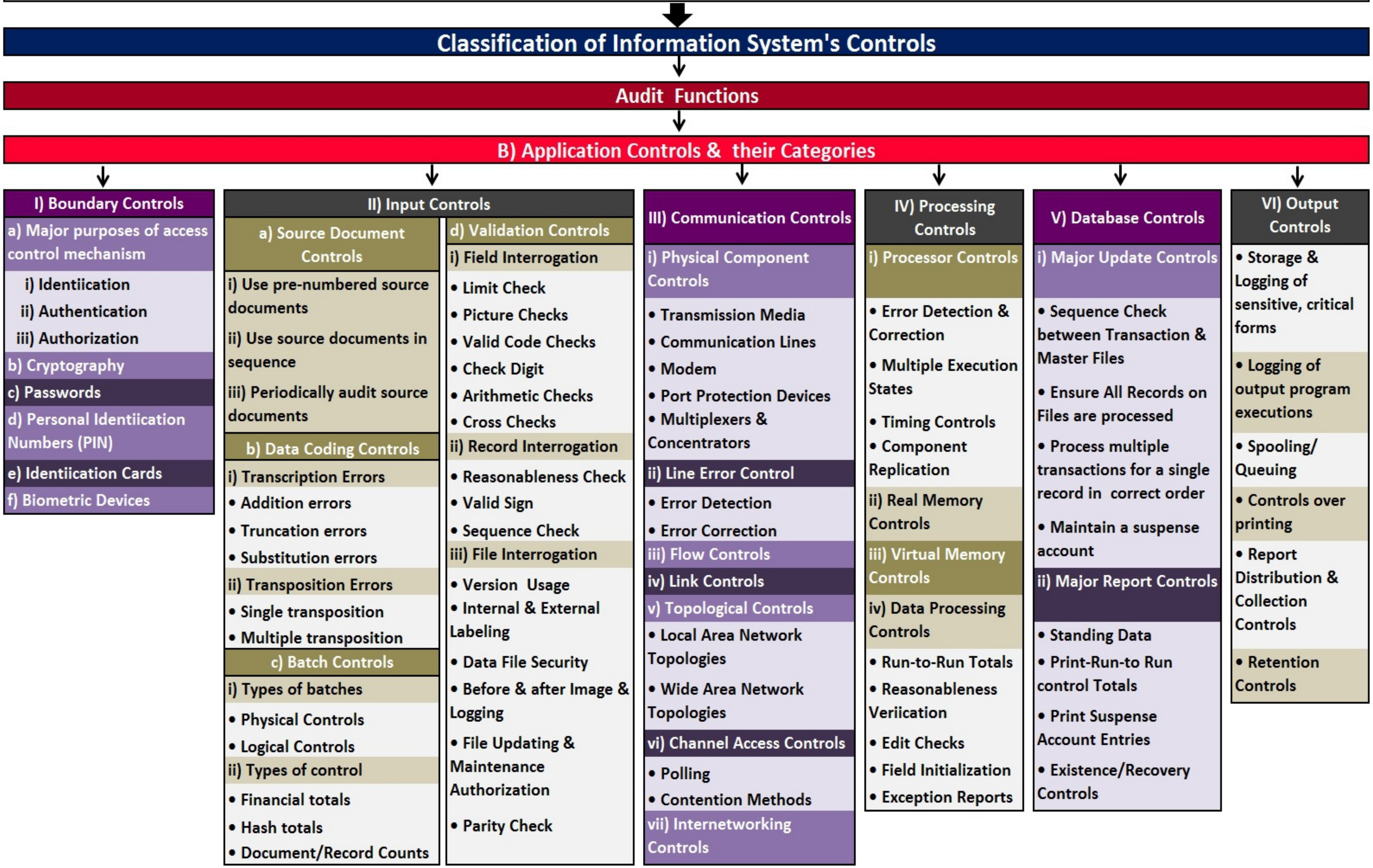
- a) Computer Operations
  - i) Operation Controls
  - ii) Scheduling Controls
  - iii) Maintenance Controls
- b) Network Operations
- c) Data Preparation & Entry
- d) Production Control
- e) File Library
- f) Documentation & Program Library
- g) Help Desk/ Technical support
- h) Capacity Planning &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

VII) Systems Development Management Controls

- a) System Authorization Activities
- b) User Speciication Activities
- c) Technical Design Activities
- d) Internal Auditor's Participation
- e) Program Testing
- f) User Test & Acceptance Procedures

(Continue on Chart 3.75)

INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.75)



Classification of Information System's Controls

Audit Functions

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

i) Types of batches

- Physical Controls
- Logical Controls

ii) Types of control

- Financial totals
- Hash totals
- Document/Record Counts

d) Validation Controls

i) Field Interrogation

- Limit Check
- Picture Checks
- Valid Code Checks
- Check Digit
- Arithmetic 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 Veriication
- 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

INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.76)

Information System Auditing

Objectives

1) Asset Safeguarding Objectives
2) Data Integrity Objectives
3) System Effectiveness Objectives
4) System Eficiency Objectives

Need for Audit of IS

1) Organisational Costs of Data Loss
2) Cost of Incorrect Decision Making
3) Costs of Computer Abuse
4) Value of Computer Hardware, Software & Personnel
5) High Costs of Computer Error
7) Controlled evolution of computer Use

Types of Audit Tools

1) Snapshots
2) Integrated Test Facility (ITF)
3) System Control Audit Review File (SCARF)
4) Continuous & Intermittent Simulation (CIS)
5) Audit Hooks

IS Audit & Audit Evidence

1) Means of controlling current audit work
2) Evidence of audit work performed
3) Schedules supporting or additional item in accounts
4) Information about business being audited, including recent history

Inherent Limitations of Audit

1) Nature of financial reporting
2) Nature of audit procedures
3) Need for audit to be conducted within a reasonable period of time & at a reasonable cost
4) Matter of difficulty, time, or cost involved is not in itself a valid basis for auditor
5) Fraud, particularly fraud involving senior management or collusion
6) Existence & completeness of related party relationships & trans.
7) Occurrence of non-compliance with laws & regulations
8) Future events or conditions that may cause an entity to cease to continue as a going concern

Segregation of Duties

It ensures that single individuals do not possess excess privileges that could result in unauthorized activities such as fraud or manipulation or exposure of sensitive data

Examples of Segregation of Duties Controls

1) Transaction Authorization
2) Split custody of high-value
3) Worklow
4) Periodic reviews

The choices for mitigating a SOD issue include

1) Reduce access privileges
2) Introduce a new mitigating control

Organizations Structure & Responsibility

1) Short & long-term objectives

i) Market conditions
ii) Regulation
iii) Available talent

2) Roles & Responsibilities

It defines specific job titles & duties, & it denotes generic expectations & responsibilities regarding use & protection of assets

3) Individual Roles & Responsibilities

i) Executive management
ii) Owner
iii) Manager
iv) User

4) Job Titles & Job Descriptions

i) Job titles in IT have matured & are quite consistent across organizations. This consistency helps organizations in several ways

- Recruiting
- Career advancement
- Compensation baselining

ii) Additional titles such as district manager, group manager, or area manager

a) Executive Management
- CIO
- CTO
- CSO
- CISO
- CPO

b) Software Development
- Systems Architect
- Systems Analyst
- Software Developer, Programmer
- Software Tester

c) Data Management
- Database Architect
- Database Administrator (DBA)
- Database Analyst

d) Network Management
- Network Architect
- Network Engineer
- Network Administrator
- Telecom Engineer

e) Systems Management
- Systems Architect
- Systems Engineer
- Storage Engineer
- Systems Administrator

f) General Operations
- Operations Manager
- Operations Analyst
- Controls Analyst
- Systems Operator
- Data Entry
- Media Librarian

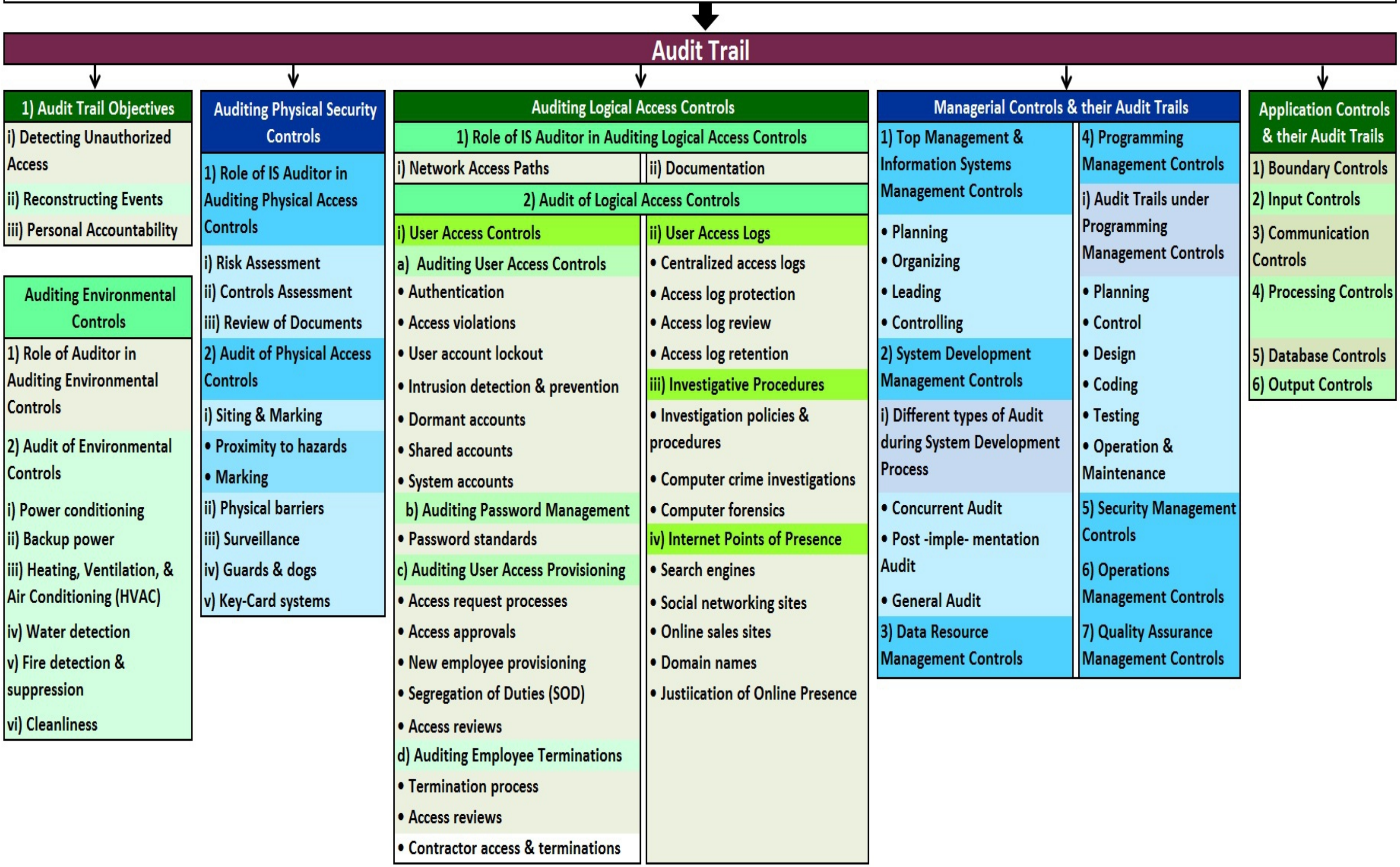
g) Security Operations
- Security Architect
- Security Engineer
- Security Analyst
- User Account Management
- Security Auditor

SP CLASSES
For CA -CPT, IPCC & FINAL
Since 2010
your Success Point

Designed By: Swapnil Patni
- CA, CS, LLB, B.Com., CISA
- Expertise knowledge in ISCA, IT, SM, LAW
- Presence all over India at the age of 29
- Also known as the "Motivational Guru"

Team SPC

INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.77)



Audit Trail

1) Audit Trail Objectives
- i) Detecting Unauthorized Access
- ii) Reconstructing Events
- iii) Personal Accountability

Auditing Environmental Controls
1) Role of Auditor in Auditing Environmental Controls

2) Audit of Environmental Controls
- i) Power conditioning
- ii) Backup power
- iii) Heating, Ventilation, & Air Conditioning (HVAC)
- iv) Water detection
- v) Fire detection & suppression
- vi) Cleanliness

Auditing Physical Security Controls
1) Role of IS Auditor in Auditing Physical Access Controls
- i) Risk Assessment
- ii) Controls Assessment
- iii) Review of Documents

2) Audit of Physical Access Controls
- i) Siting & Marking
  - Proximity to hazards
  - Marking
- ii) Physical barriers
- iii) Surveillance
- iv) Guards & dogs
- v) Key-Card systems

Auditing Logical Access Controls
1) Role of IS Auditor in Auditing Logical Access Controls
- i) Network Access Paths
- ii) Documentation

2) Audit of Logical Access Controls

i) User Access Controls

a) Auditing User Access Controls
- Authentication
- Access violations
- User account lockout
- Intrusion detection & prevention
- Dormant accounts
- Shared accounts
- System accounts

b) Auditing Password Management
- Password standards

c) Auditing User Access Provisioning
- Access request processes
- Access approvals
- New employee provisioning
- Segregation of Duties (SOD)
- Access reviews

d) Auditing Employee Terminations
- Termination process
- Access reviews
- Contractor access & terminations

ii) User Access Logs
- Centralized access logs
- Access log protection
- Access log review
- Access log retention

iii) Investigative Procedures
- Investigation policies & procedures
- Computer crime investigations
- Computer forensics

iv) Internet Points of Presence
- Search engines
- Social networking sites
- Online sales sites
- Domain names
- Justiication of Online Presence

Managerial Controls & their Audit Trails
1) Top Management & Information Systems Management Controls
- Planning
- Organizing
- Leading
- Controlling

2) System Development Management Controls

i) Different types of Audit during System Development Process
- Concurrent Audit
- Post -imple- mentation Audit
- General Audit

3) Data Resource Management Controls

4) Programming Management Controls

i) Audit Trails under Programming Management Controls
- Planning
- Control
- Design
- Coding
- Testing
- Operation & Maintenance

5) Security Management Controls

6) Operations Management Controls

7) Quality Assurance Management Controls

Application Controls & their Audit Trails
1) Boundary Controls

2) Input Controls

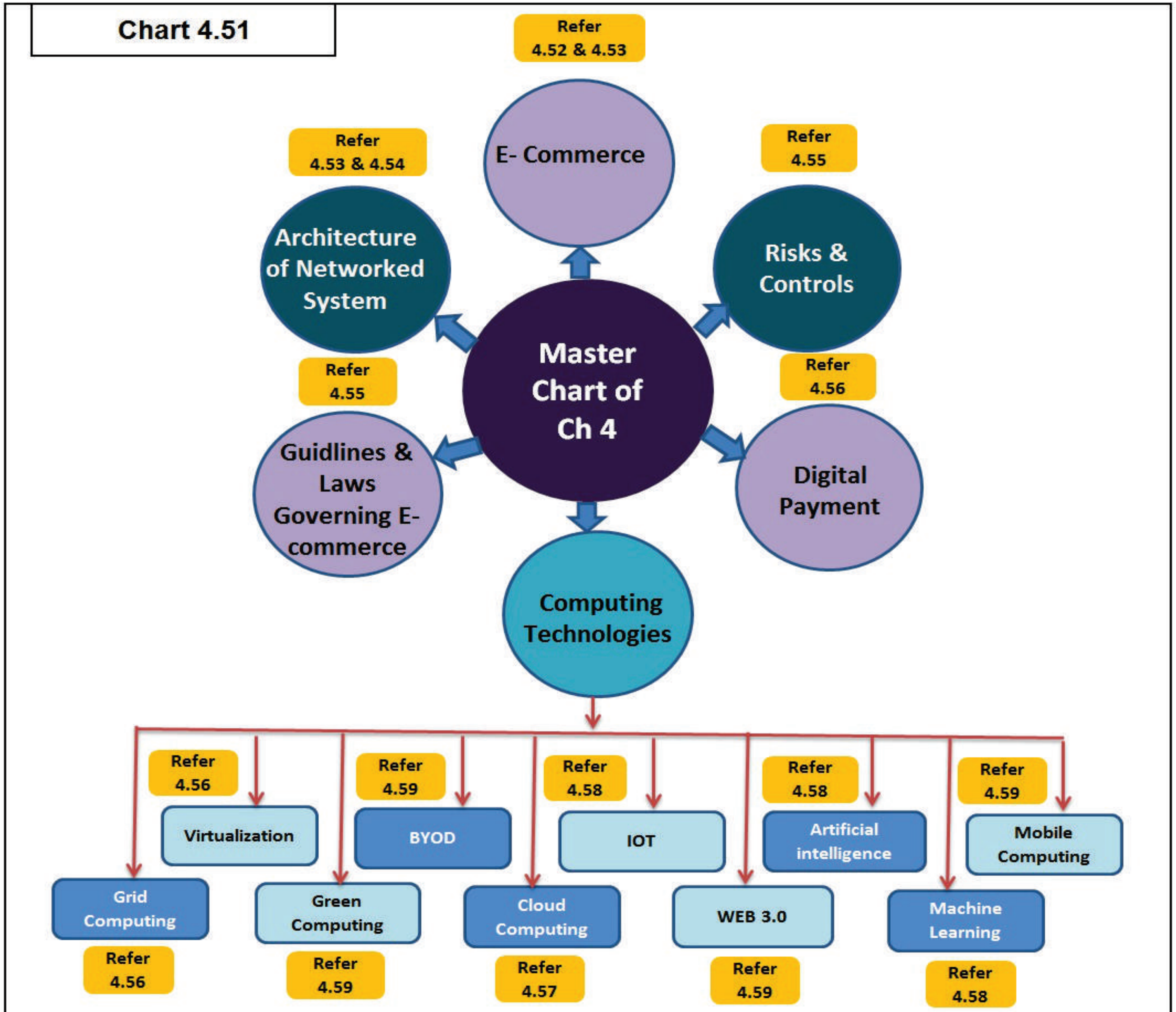
3) Communication Controls

4) Processing Controls

5) Database Controls

6) Output Controls

Chart 4.51



Master Chart of Ch 4

E- Commerce
Refer 4.52 & 4.53

Architecture of Networked System
Refer 4.53 & 4.54

Risks & Controls
Refer 4.55

Guidlines & Laws Governing E-commerce
Refer 4.55

Digital Payment
Refer 4.56

Computing Technologies

Grid Computing
Refer 4.56

Virtualization
Refer 4.56

Green Computing
Refer 4.59

BYOD
Refer 4.59

Cloud Computing
Refer 4.57

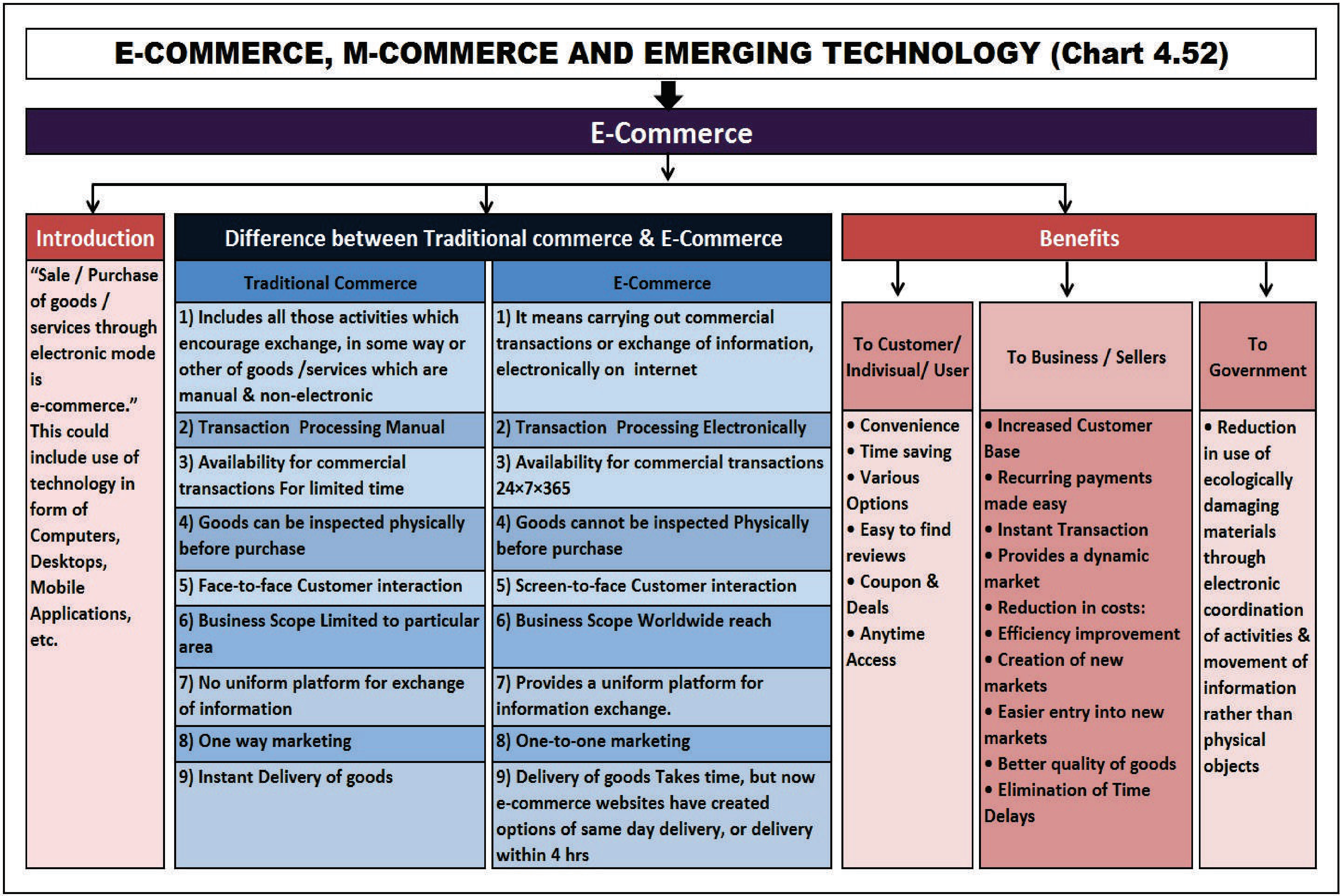
IOT
Refer 4.58

WEB 3.0
Refer 4.59

Artificial intelligence
Refer 4.58

Machine Learning
Refer 4.58

Mobile Computing
Refer 4.59



E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.52)

E-Commerce

Introduction

"Sale / Purchase of goods / services through electronic mode is e-commerce." This could include use of technology in form of Computers, Desktops, Mobile Applications, etc.

Difference between Traditional commerce & E-Commerce

Traditional Commerce	E-Commerce
1) Includes all those activities which encourage exchange, in some way or other of goods /services which are manual & non-electronic	1) It means carrying out commercial transactions or exchange of information, electronically on internet
2) Transaction Processing Manual	2) Transaction Processing Electronically
3) Availability for commercial transactions For limited time	3) Availability for commercial transactions 24×7×365
4) Goods can be inspected physically before purchase	4) Goods cannot be inspected Physically before purchase
5) Face-to-face Customer interaction	5) Screen-to-face Customer interaction
6) Business Scope Limited to particular area	6) Business Scope Worldwide reach
7) No uniform platform for exchange of information	7) Provides a uniform platform for information exchange.
8) One way marketing	8) One-to-one marketing
9) Instant Delivery of goods	9) Delivery of goods Takes time, but now e-commerce websites have created options of same day delivery, or delivery within 4 hrs

Benefits

To Customer/ Indivisual/ User

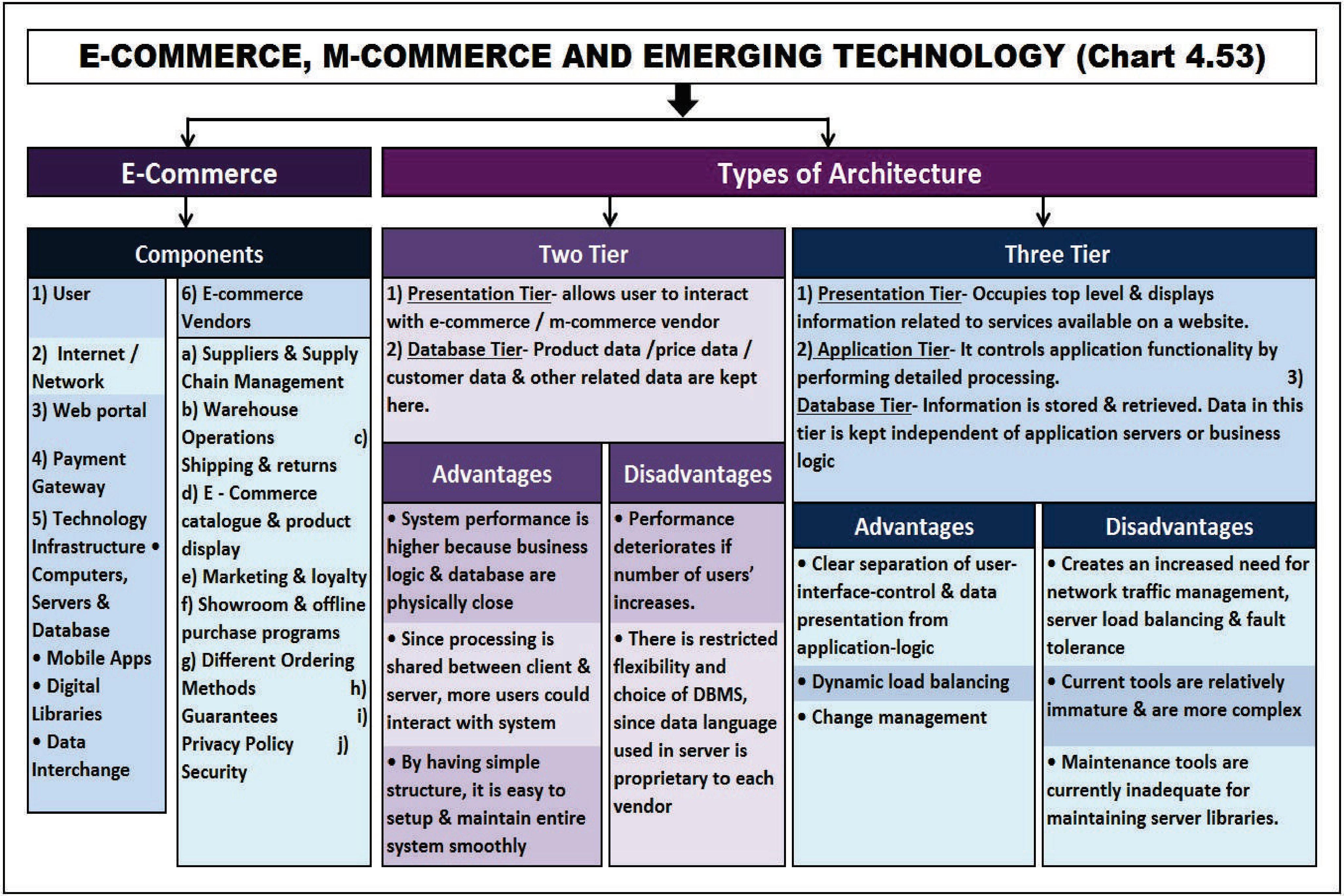
- Convenience
- Time saving
- Various Options
- Easy to find reviews
- Coupon & Deals
- Anytime Access

To Business / Sellers

- Increased Customer Base
- Recurring payments made easy
- Instant Transaction
- Provides a dynamic market
- Reduction in costs:
- Efficiency improvement
- Creation of new markets
- Easier entry into new markets
- Better quality of goods
- Elimination of Time Delays

To Government

- Reduction in use of ecologically damaging materials through electronic coordination of activities & movement of information rather than physical objects



E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.53)

E-Commerce

Components

1) User

2) Internet / Network

3) Web portal

4) Payment Gateway

5) Technology Infrastructure • Computers, Servers & Database
- Mobile Apps
- Digital Libraries
- Data Interchange

6) E-commerce Vendors

a) Suppliers & Supply Chain Management b) Warehouse Operations c) Shipping & returns d) E - Commerce catalogue & product display e) Marketing & loyalty f) Showroom & offline purchase programs g) Different Ordering Methods h) Guarantees i) Privacy Policy j) Security

Types of Architecture

Two Tier

1) Presentation Tier- allows user to interact with e-commerce / m-commerce vendor

2) Database Tier- Product data /price data / customer data & other related data are kept here.

Advantages

- System performance is higher because business logic & database are physically close
- Since processing is shared between client & server, more users could interact with system
- By having simple structure, it is easy to setup & maintain entire system smoothly

Disadvantages

- Performance deteriorates if number of users' increases.
- There is restricted flexibility and choice of DBMS, since data language used in server is proprietary to each vendor

Three Tier

1) Presentation Tier- Occupies top level & displays information related to services available on a website.

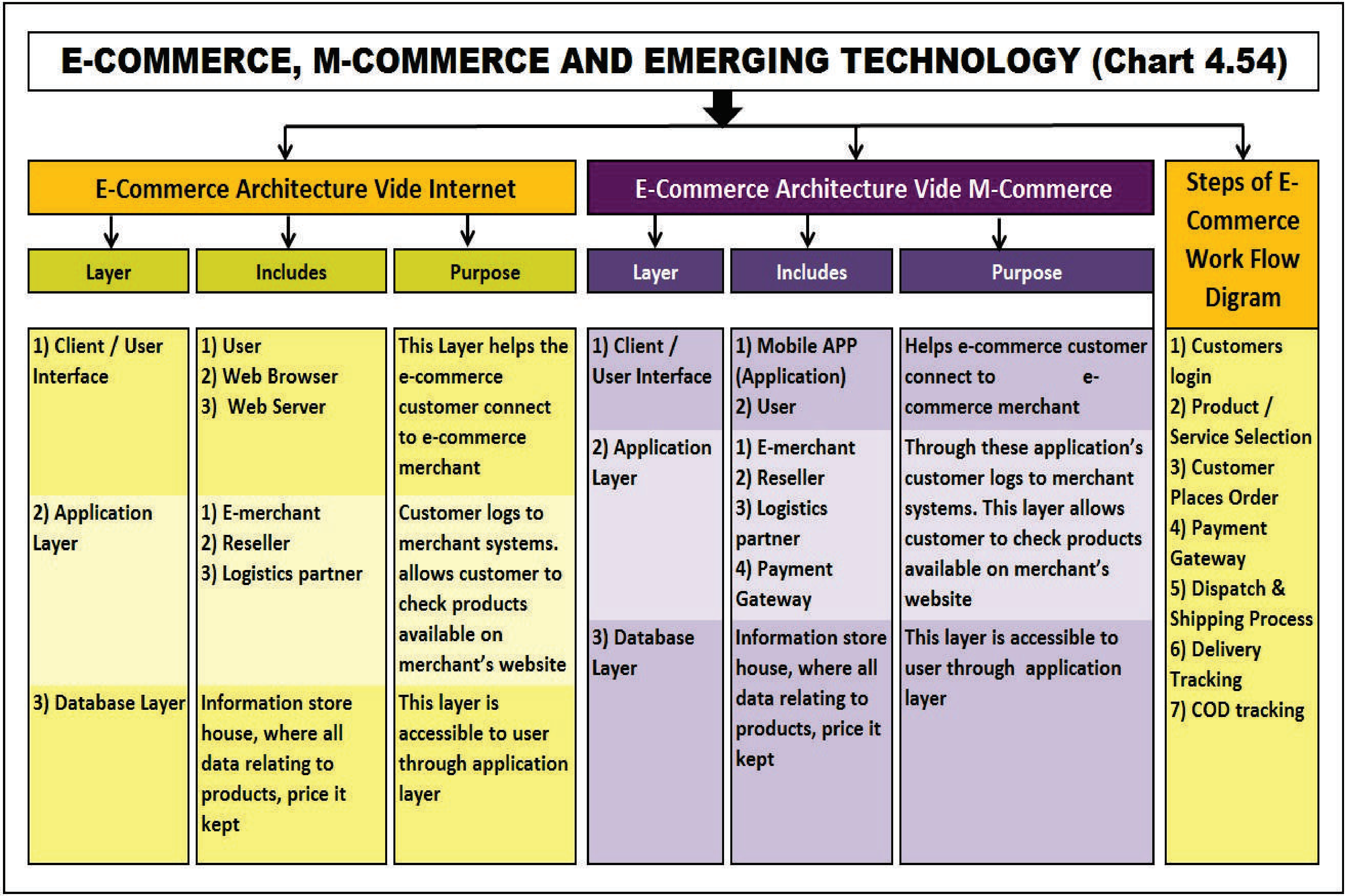
2) Application Tier- It controls application functionality by performing detailed processing. 3) Database Tier- Information is stored & retrieved. Data in this tier is kept independent of application servers or business logic

Advantages

- Clear separation of user-interface-control & data presentation from application-logic
- Dynamic load balancing
- Change management

Disadvantages

- Creates an increased need for network traffic management, server load balancing & fault tolerance
- Current tools are relatively immature & are more complex
- Maintenance tools are currently inadequate for maintaining server libraries.



E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.54)

E-Commerce Architecture Vide Internet

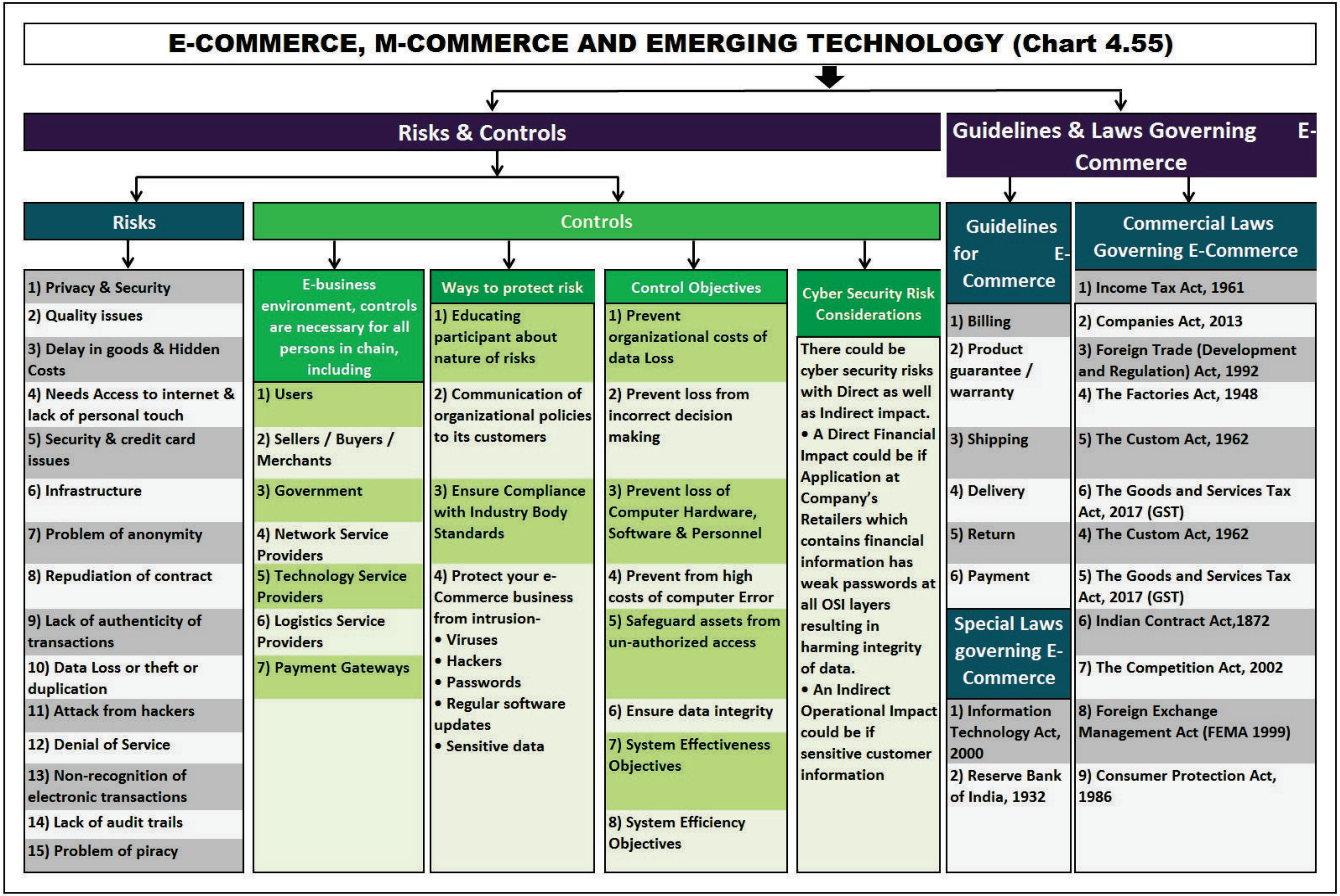
Layer	Includes	Purpose
1) Client / User Interface	1) User 2) Web Browser 3) Web Server	This Layer helps the e-commerce customer connect to e-commerce merchant
2) Application Layer	1) E-merchant 2) Reseller 3) Logistics partner	Customer logs to merchant systems. allows customer to check products available on merchant's website
3) Database Layer	Information store house, where all data relating to products, price it kept	This layer is accessible to user through application layer

E-Commerce Architecture Vide M-Commerce

Layer	Includes	Purpose
1) Client / User Interface	1) Mobile APP (Application) 2) User	Helps e-commerce customer connect to e-commerce merchant
2) Application Layer	1) E-merchant 2) Reseller 3) Logistics partner 4) Payment Gateway	Through these application's customer logs to merchant systems. This layer allows customer to check products available on merchant's website
3) Database Layer	Information store house, where all data relating to products, price it kept	This layer is accessible to user through application layer

Steps of E-Commerce Work Flow Digram

1) Customers login
2) Product / Service Selection
3) Customer Places Order
4) Payment Gateway
5) Dispatch & Shipping Process
6) Delivery Tracking
7) COD tracking



E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.55)

Risks & Controls

Risks

1) Privacy & Security
2) Quality issues
3) Delay in goods & Hidden Costs
4) Needs Access to internet & lack of personal touch
5) Security & credit card issues
6) Infrastructure
7) Problem of anonymity
8) Repudiation of contract
9) Lack of authenticity of transactions
10) Data Loss or theft or duplication
11) Attack from hackers
12) Denial of Service
13) Non-recognition of electronic transactions
14) Lack of audit trails
15) Problem of piracy

Controls

E-business environment, controls are necessary for all persons in chain, including

1) Users
2) Sellers / Buyers / Merchants
3) Government
4) Network Service Providers
5) Technology Service Providers
6) Logistics Service Providers
7) Payment Gateways

Ways to protect risk

1) Educating participant about nature of risks
2) Communication of organizational policies to its customers
3) Ensure Compliance with Industry Body Standards
4) Protect your e-Commerce business from intrusion-
- Viruses
- Hackers
- Passwords
- Regular software updates
- Sensitive data

Control Objectives

1) Prevent organizational costs of data Loss
2) Prevent loss from incorrect decision making
3) Prevent loss of Computer Hardware, Software & Personnel
4) Prevent from high costs of computer Error
5) Safeguard assets from un-authorized access
6) Ensure data integrity
7) System Effectiveness Objectives
8) System Efficiency Objectives

Cyber Security Risk Considerations

There could be cyber security risks with Direct as well as Indirect impact.

- A Direct Financial Impact could be if Application at Company's Retailers which contains financial information has weak passwords at all OSI layers resulting in harming integrity of data.
- An Indirect Operational Impact could be if sensitive customer information

Guidelines & Laws Governing E-Commerce

Guidelines for E-Commerce

1) Billing
2) Product guarantee / warranty
3) Shipping
4) Delivery
5) Return
6) Payment

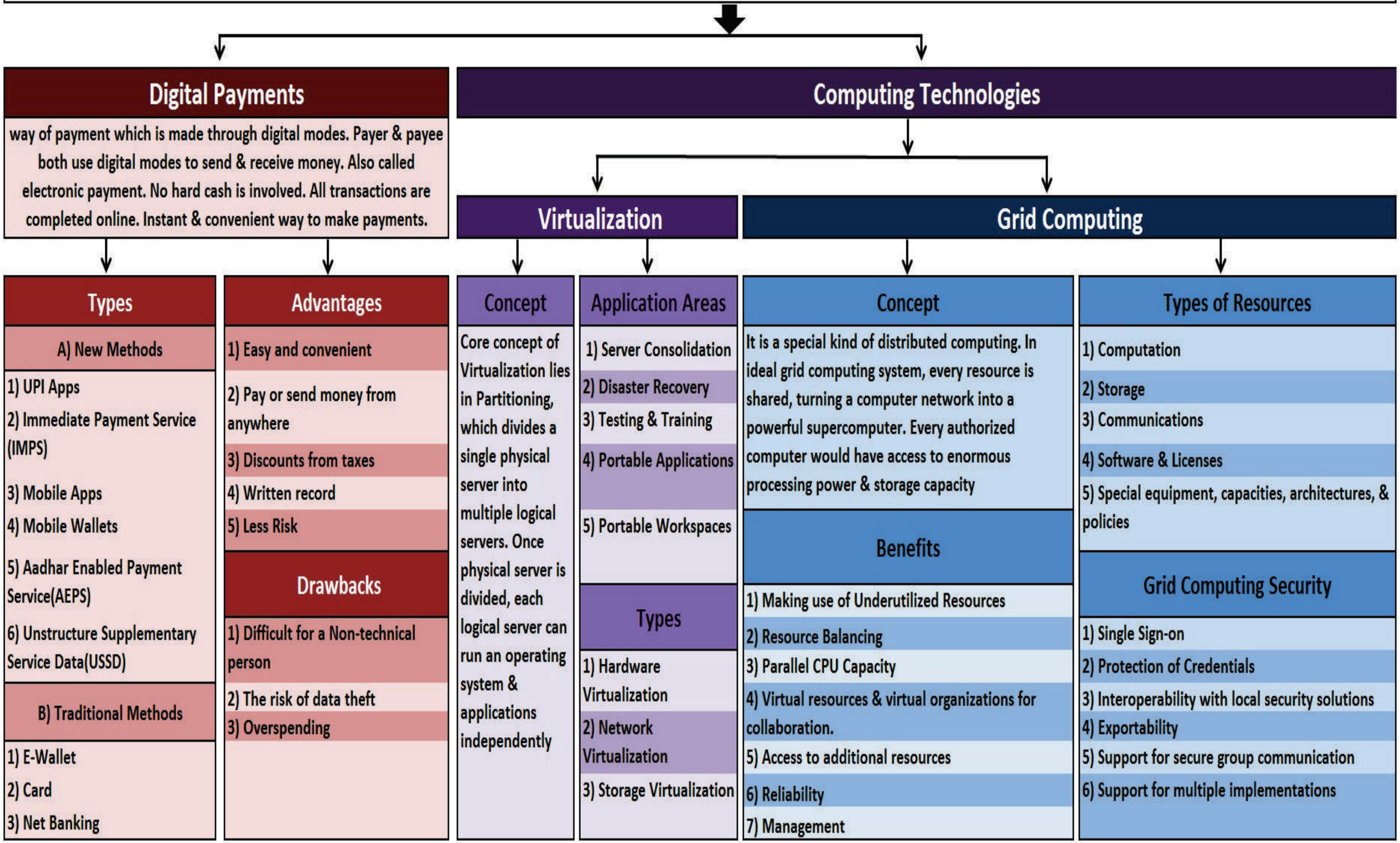
Special Laws governing E-Commerce

1) Information Technology Act, 2000
2) Reserve Bank of India, 1932

Commercial Laws Governing E-Commerce

1) Income Tax Act, 1961
2) Companies Act, 2013
3) Foreign Trade (Development and Regulation) Act, 1992
4) The Factories Act, 1948
5) The Custom Act, 1962
6) The Goods and Services Tax Act, 2017 (GST)
4) The Custom Act, 1962
5) The Goods and Services Tax Act, 2017 (GST)
6) Indian Contract Act,1872
7) The Competition Act, 2002
8) Foreign Exchange Management Act (FEMA 1999)
9) Consumer Protection Act, 1986

E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.56)



Digital Payments

way of payment which is made through digital modes. Payer & payee both use digital modes to send & receive money. Also called electronic payment. No hard cash is involved. All transactions are completed online. Instant & convenient way to make payments.

Types

A) New Methods

1) UPI Apps
2) Immediate Payment Service (IMPS)
3) Mobile Apps
4) Mobile Wallets
5) Aadhar Enabled Payment Service(AEPS)
6) Unstructure Supplementary Service Data(USSD)

B) Traditional Methods

1) E-Wallet
2) Card
3) Net Banking

Advantages

1) Easy and convenient
2) Pay or send money from anywhere
3) Discounts from taxes
4) Written record
5) Less Risk

Drawbacks

1) Difficult for a Non-technical person
2) The risk of data theft
3) Overspending

Computing Technologies

Virtualization

Concept

Core concept of Virtualization lies in Partitioning, which divides a single physical server into multiple logical servers. Once physical server is divided, each logical server can run an operating system & applications independently

Application Areas

1) Server Consolidation
2) Disaster Recovery
3) Testing & Training
4) Portable Applications
5) Portable Workspaces

Types

1) Hardware Virtualization
2) Network Virtualization
3) Storage Virtualization

Grid Computing

Concept

It is a special kind of distributed computing. In ideal grid computing system, every resource is shared, turning a computer network into a powerful supercomputer. Every authorized computer would have access to enormous processing power & storage capacity

Benefits

1) Making use of Underutilized Resources
2) Resource Balancing
3) Parallel CPU Capacity
4) Virtual resources & virtual organizations for collaboration.
5) Access to additional resources
6) Reliability
7) Management

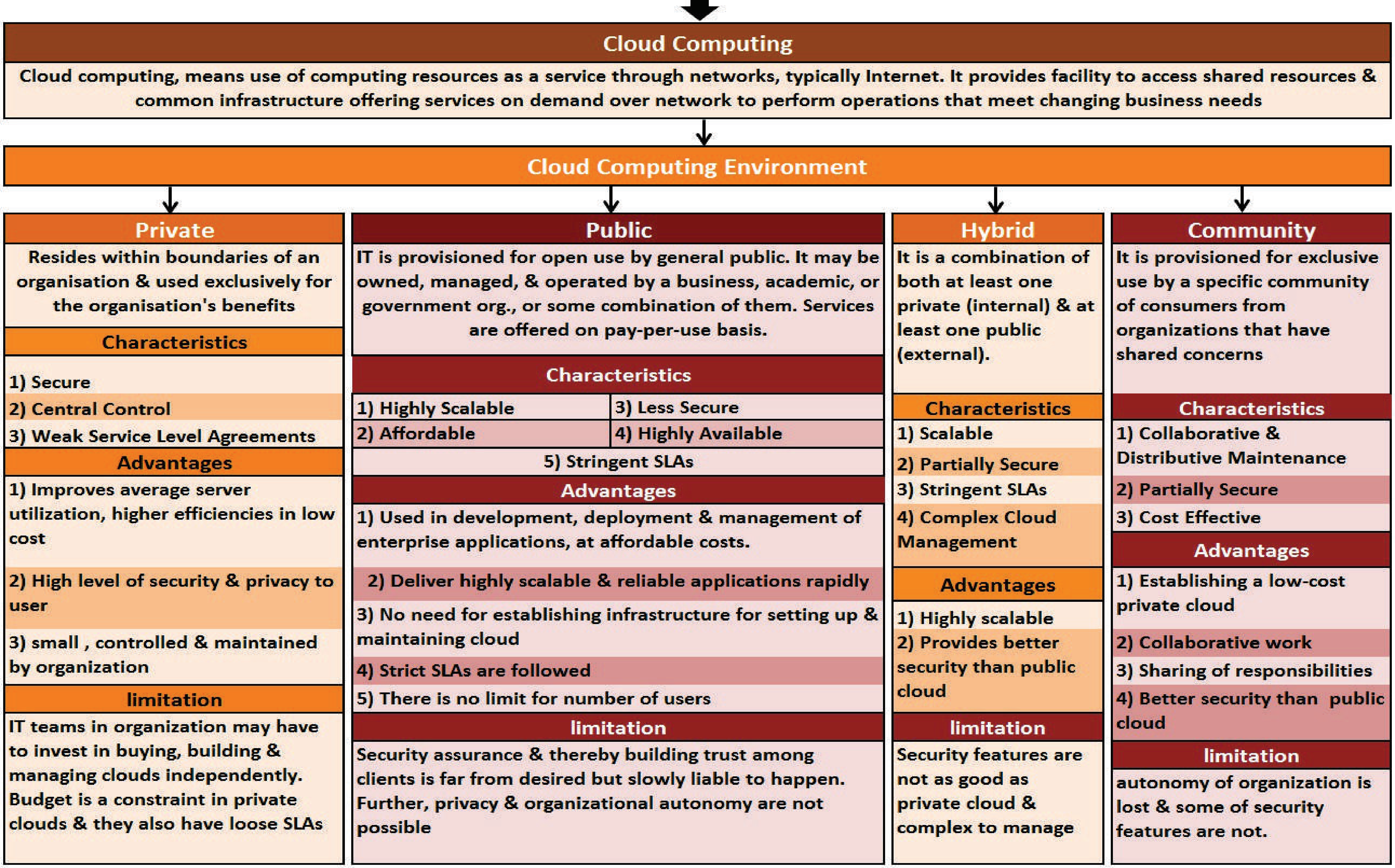
Types of Resources

1) Computation
2) Storage
3) Communications
4) Software & Licenses
5) Special equipment, capacities, architectures, & policies

Grid Computing Security

1) Single Sign-on
2) Protection of Credentials
3) Interoperability with local security solutions
4) Exportability
5) Support for secure group communication
6) Support for multiple implementations

E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.57)



Cloud Computing

Cloud computing, means use of computing resources as a service through networks, typically Internet. It provides facility to access shared resources & common infrastructure offering services on demand over network to perform operations that meet changing business needs

Cloud Computing Environment

Private

Resides within boundaries of an organisation & used exclusively for the organisation's benefits

Characteristics

1) Secure
2) Central Control
3) Weak Service Level Agreements

Advantages

1) Improves average server utilization, higher efficiencies in low cost
2) High level of security & privacy to user
3) small , controlled & maintained by organization

limitation

IT teams in organization may have to invest in buying, building & managing clouds independently. Budget is a constraint in private clouds & they also have loose SLAs

Public

IT is provisioned for open use by general public. It may be owned, managed, & operated by a business, academic, or government org., or some combination of them. Services are offered on pay-per-use basis.

Characteristics

1) Highly Scalable
2) Affordable
3) Less Secure
4) Highly Available
5) Stringent SLAs

Advantages

1) Used in development, deployment & management of enterprise applications, at affordable costs.
2) Deliver highly scalable & reliable applications rapidly
3) No need for establishing infrastructure for setting up & maintaining cloud
4) Strict SLAs are followed
5) There is no limit for number of users

limitation

Security assurance & thereby building trust among clients is far from desired but slowly liable to happen. Further, privacy & organizational autonomy are not possible

Hybrid

It is a combination of both at least one private (internal) & at least one public (external).

Characteristics

1) Scalable
2) Partially Secure
3) Stringent SLAs
4) Complex Cloud Management

Advantages

1) Highly scalable
2) Provides better security than public cloud

limitation

Security features are not as good as private cloud & complex to manage

Community

It is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns

Characteristics

1) Collaborative & Distributive Maintenance
2) Partially Secure
3) Cost Effective

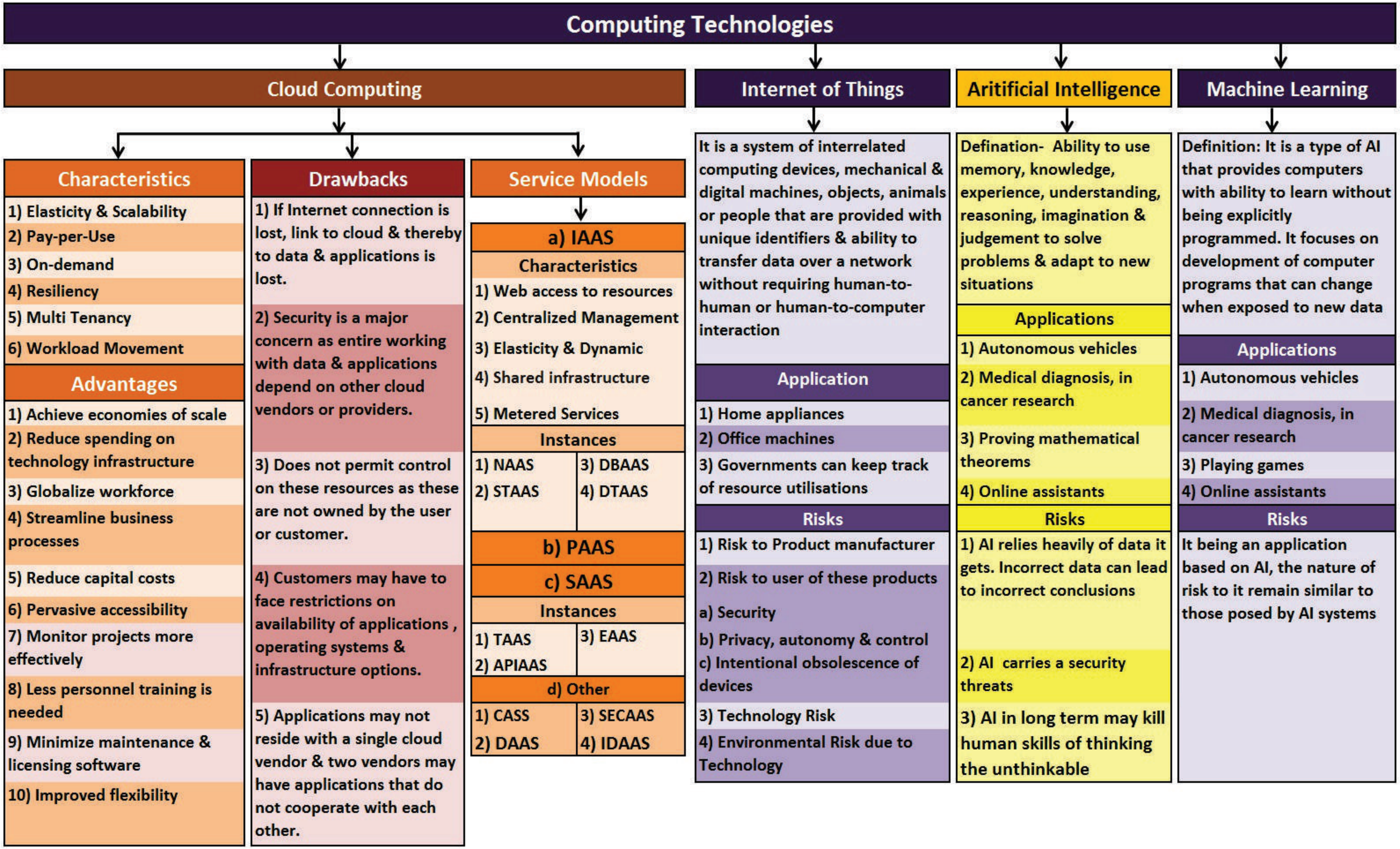
Advantages

1) Establishing a low-cost private cloud
2) Collaborative work
3) Sharing of responsibilities
4) Better security than public cloud

limitation

autonomy of organization is lost & some of security features are not.

E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.58)



Computing Technologies

Cloud Computing

Characteristics

1) Elasticity & Scalability
2) Pay-per-Use
3) On-demand
4) Resiliency
5) Multi Tenancy
6) Workload Movement

Advantages

1) Achieve economies of scale
2) Reduce spending on technology infrastructure
3) Globalize workforce
4) Streamline business processes
5) Reduce capital costs
6) Pervasive accessibility
7) Monitor projects more effectively
8) Less personnel training is needed
9) Minimize maintenance & licensing software
10) Improved flexibility

Drawbacks

1) If Internet connection is lost, link to cloud & thereby to data & applications is lost.
2) Security is a major concern as entire working with data & applications depend on other cloud vendors or providers.
3) Does not permit control on these resources as these are not owned by the user or customer.
4) Customers may have to face restrictions on availability of applications , operating systems & infrastructure options.
5) Applications may not reside with a single cloud vendor & two vendors may have applications that do not cooperate with each other.

Service Models

a) IAAS

Characteristics

1) Web access to resources
2) Centralized Management
3) Elasticity & Dynamic
4) Shared infrastructure
5) Metered Services

Instances

1) NAAS	3) DBAAS
2) STAAS	4) DTAAS

b) PAAS

c) SAAS

Instances

1) TAAS	3) EAAS
2) APIAAS	

d) Other

1) CASS	3) SECAAS
2) DAAS	4) IDAAS

Internet of Things

It is a system of interrelated computing devices, mechanical & digital machines, objects, animals or people that are provided with unique identifiers & ability to transfer data over a network without requiring human-to-human or human-to-computer interaction

Application

1) Home appliances
2) Office machines
3) Governments can keep track of resource utilisations

Risks

1) Risk to Product manufacturer
2) Risk to user of these products

a) Security
b) Privacy, autonomy & control
c) Intentional obsolescence of devices

3) Technology Risk
4) Environmental Risk due to Technology

Aritificial Intelligence

Defination- Ability to use memory, knowledge, experience, understanding, reasoning, imagination & judgement to solve problems & adapt to new situations

Applications

1) Autonomous vehicles
2) Medical diagnosis, in cancer research
3) Proving mathematical theorems
4) Online assistants

Risks

1) AI relies heavily of data it gets. Incorrect data can lead to incorrect conclusions
2) AI carries a security threats
3) AI in long term may kill human skills of thinking the unthinkable

Machine Learning

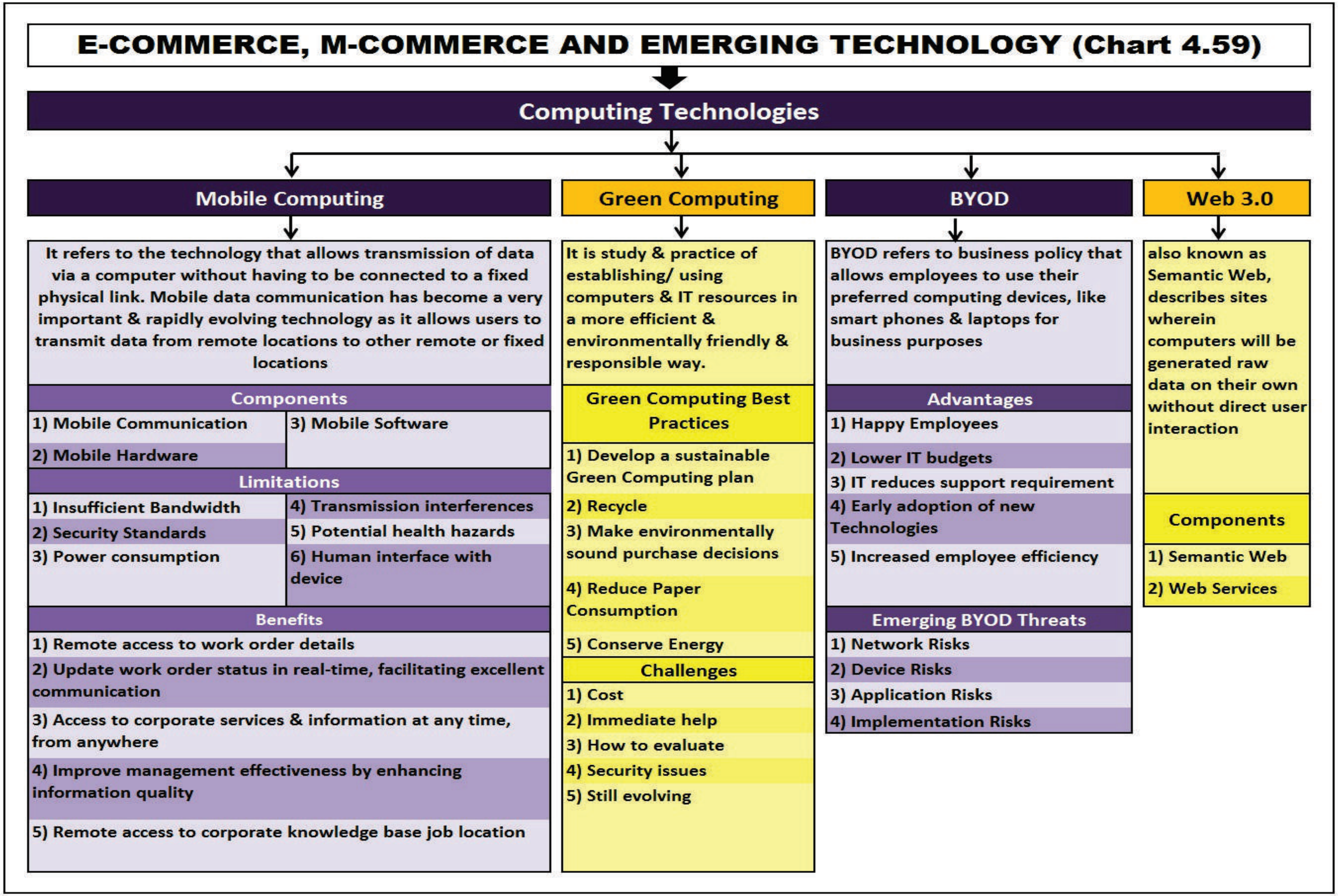
Definition: It is a type of AI that provides computers with ability to learn without being explicitly programmed. It focuses on development of computer programs that can change when exposed to new data

Applications

1) Autonomous vehicles
2) Medical diagnosis, in cancer research
3) Playing games
4) Online assistants

Risks

It being an application based on AI, the nature of risk to it remain similar to those posed by AI systems



E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.59)

Computing Technologies

Mobile Computing

It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile data communication has become a very important & rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations

Components

1) Mobile Communication
2) Mobile Hardware
3) Mobile Software

Limitations

1) Insufficient Bandwidth
2) Security Standards
3) Power consumption
4) Transmission interferences
5) Potential health hazards
6) Human interface with device

Benefits

1) Remote access to work order details
2) Update work order status in real-time, facilitating excellent communication
3) Access to corporate services & information at any time, from anywhere
4) Improve management effectiveness by enhancing information quality
5) Remote access to corporate knowledge base job location

Green Computing

It is study & practice of establishing/ using computers & IT resources in a more efficient & environmentally friendly & responsible way.

Green Computing Best Practices

1) Develop a sustainable Green Computing plan
2) Recycle
3) Make environmentally sound purchase decisions
4) Reduce Paper Consumption
5) Conserve Energy

Challenges

1) Cost
2) Immediate help
3) How to evaluate
4) Security issues
5) Still evolving

BYOD

BYOD refers to business policy that allows employees to use their preferred computing devices, like smart phones & laptops for business purposes

Advantages

1) Happy Employees
2) Lower IT budgets
3) IT reduces support requirement
4) Early adoption of new Technologies
5) Increased employee efficiency

Emerging BYOD Threats

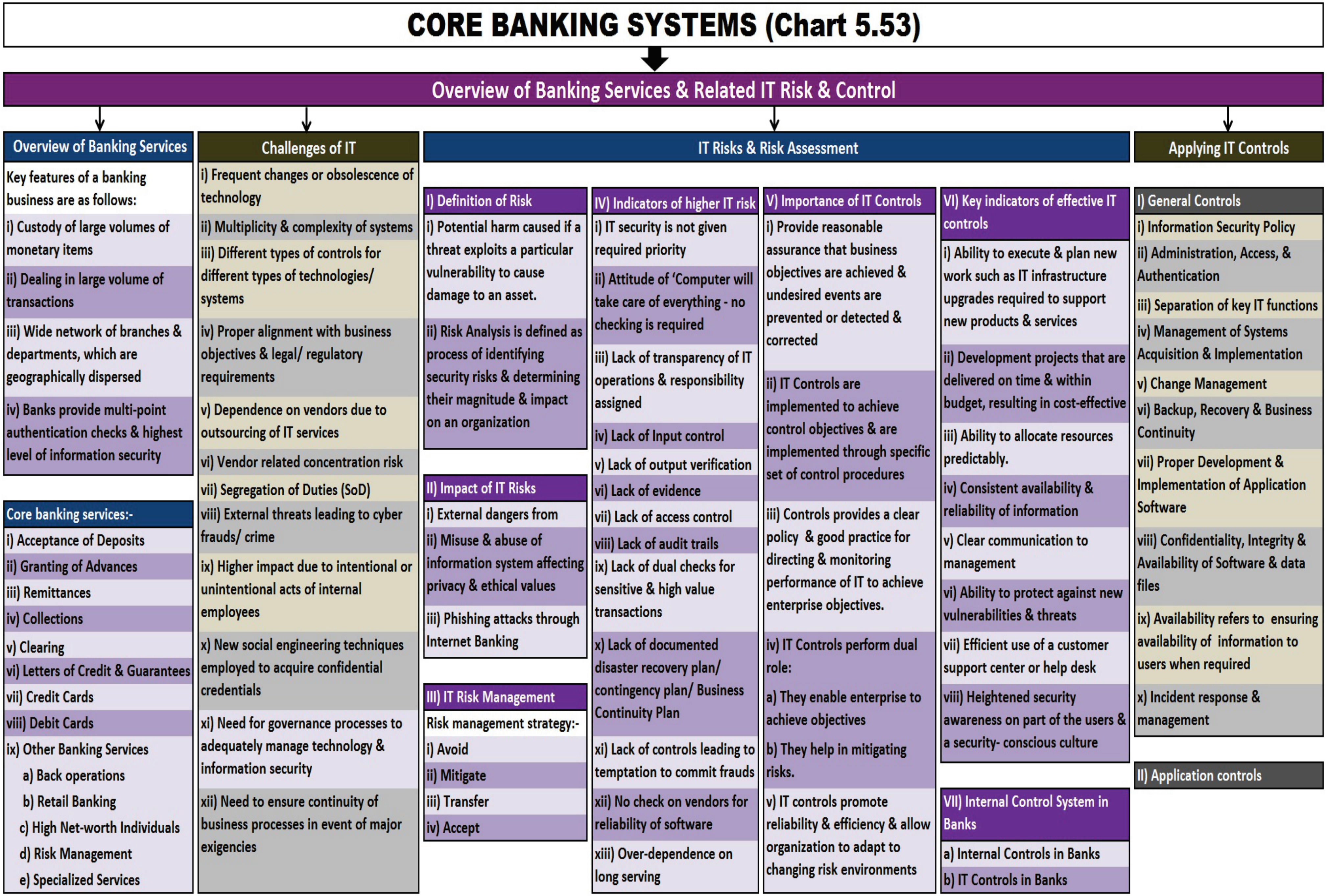
1) Network Risks
2) Device Risks
3) Application Risks
4) Implementation Risks

Web 3.0

also known as Semantic Web, describes sites wherein computers will be generated raw data on their own without direct user interaction

Components

1) Semantic Web
2) Web Services



CORE BANKING SYSTEMS (Chart 5.53)

Overview of Banking Services & Related IT Risk & Control

Overview of Banking Services

Key features of a banking business are as follows:

i) Custody of large volumes of monetary items

ii) Dealing in large volume of transactions

iii) Wide network of branches & departments, which are geographically dispersed

iv) Banks provide multi-point authentication checks & highest level of information security

Core banking services:-

i) Acceptance of Deposits

ii) Granting of Advances

iii) Remittances

iv) Collections

v) Clearing

vi) Letters of Credit & Guarantees

vii) Credit Cards

viii) Debit Cards

ix) Other Banking Services

a) Back operations

b) Retail Banking

c) High Net-worth Individuals

d) Risk Management

e) Specialized Services

Challenges of IT

i) Frequent changes or obsolescence of technology

ii) Multiplicity & complexity of systems

iii) Different types of controls for different types of technologies/ systems

iv) Proper alignment with business objectives & legal/ regulatory requirements

v) Dependence on vendors due to outsourcing of IT services

vi) Vendor related concentration risk

vii) Segregation of Duties (SoD)

viii) External threats leading to cyber frauds/ crime

ix) Higher impact due to intentional or unintentional acts of internal employees

x) New social engineering techniques employed to acquire confidential credentials

xi) Need for governance processes to adequately manage technology & information security

xii) Need to ensure continuity of business processes in event of major exigencies

IT Risks & Risk Assessment

I) Definition of Risk

i) Potential harm caused if a threat exploits a particular vulnerability to cause damage to an asset.

ii) Risk Analysis is defined as process of identifying security risks & determining their magnitude & impact on an organization

II) Impact of IT Risks

i) External dangers from

ii) Misuse & abuse of information system affecting privacy & ethical values

iii) Phishing attacks through Internet Banking

III) IT Risk Management

Risk management strategy:-

i) Avoid

ii) Mitigate

iii) Transfer

iv) Accept

IV) Indicators of higher IT risk

i) IT security is not given required priority

ii) Attitude of 'Computer will take care of everything - no checking is required

iii) Lack of transparency of IT operations & responsibility assigned

iv) Lack of Input control

v) Lack of output verification

vi) Lack of evidence

vii) Lack of access control

viii) Lack of audit trails

ix) Lack of dual checks for sensitive & high value transactions

x) Lack of documented disaster recovery plan/ contingency plan/ Business Continuity Plan

xi) Lack of controls leading to temptation to commit frauds

xii) No check on vendors for reliability of software

xiii) Over-dependence on long serving

V) Importance of IT Controls

i) Provide reasonable assurance that business objectives are achieved & undesired events are prevented or detected & corrected

ii) IT Controls are implemented to achieve control objectives & are implemented through specific set of control procedures

iii) Controls provides a clear policy & good practice for directing & monitoring performance of IT to achieve enterprise objectives.

iv) IT Controls perform dual role:

a) They enable enterprise to achieve objectives

b) They help in mitigating risks.

v) IT controls promote reliability & efficiency & allow organization to adapt to changing risk environments

VI) Key indicators of effective IT controls

i) Ability to execute & plan new work such as IT infrastructure upgrades required to support new products & services

ii) Development projects that are delivered on time & within budget, resulting in cost-effective

iii) Ability to allocate resources predictably.

iv) Consistent availability & reliability of information

v) Clear communication to management

vi) Ability to protect against new vulnerabilities & threats

vii) Efficient use of a customer support center or help desk

viii) Heightened security awareness on part of the users & a security- conscious culture

VII) Internal Control System in Banks

a) Internal Controls in Banks

b) IT Controls in Banks

Applying IT Controls

I) General Controls

i) Information Security Policy

ii) Administration, Access, & Authentication

iii) Separation of key IT functions

iv) Management of Systems Acquisition & Implementation

v) Change Management

vi) Backup, Recovery & Business Continuity

vii) Proper Development & Implementation of Application Software

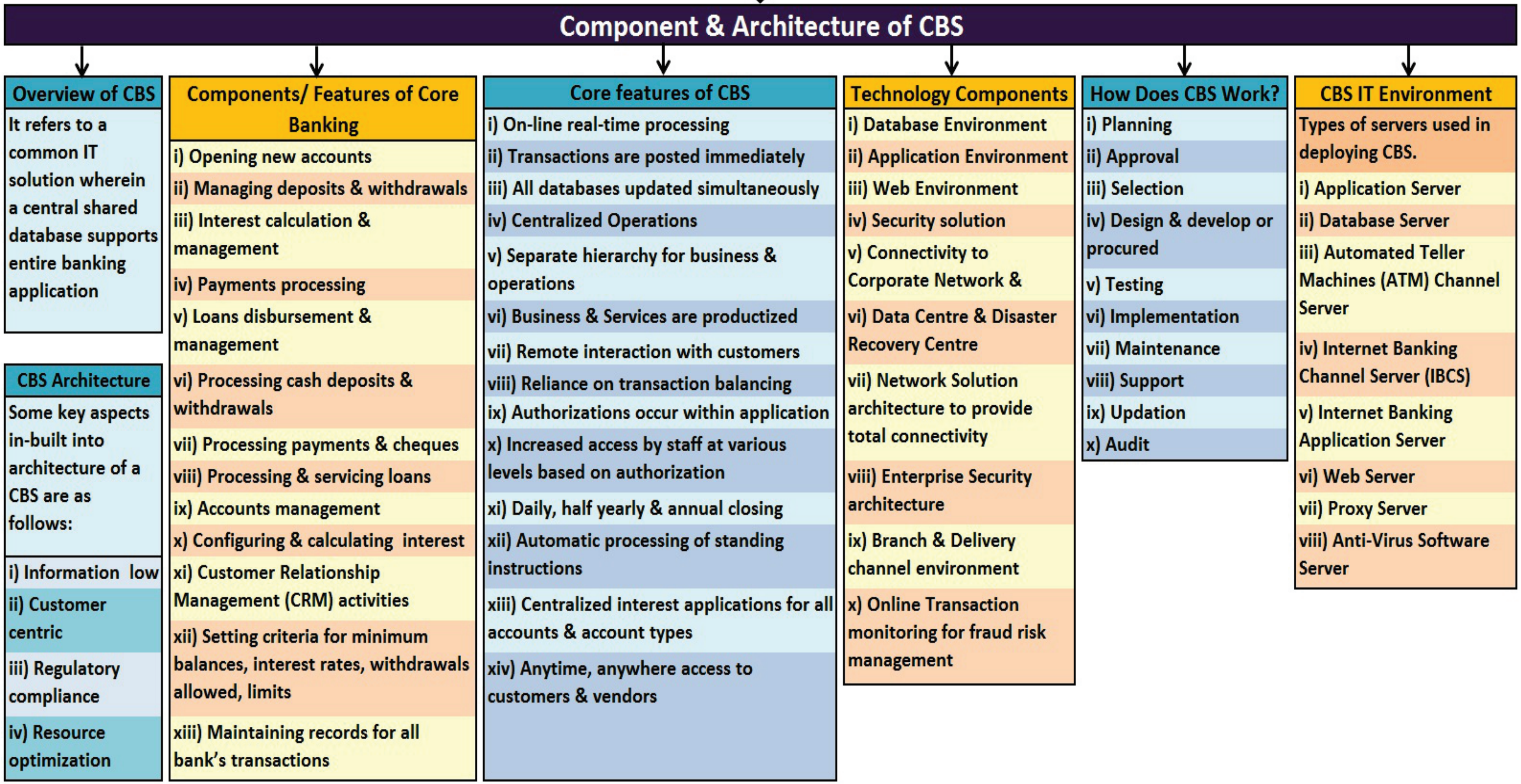
viii) Confidentiality, Integrity & Availability of Software & data files

ix) Availability refers to ensuring availability of information to users when required

x) Incident response & management

II) Application controls

CORE BANKING SYSTEMS (Chart 5.54)



Component & Architecture of CBS

Overview of CBS

It refers to a common IT solution wherein a central shared database supports entire banking application

CBS Architecture

Some key aspects in-built into architecture of a CBS are as follows:

- i) Information low
- ii) Customer centric
- iii) Regulatory compliance
- iv) Resource optimization

Components/ Features of Core Banking

- i) Opening new accounts
- ii) Managing deposits & withdrawals
- iii) Interest calculation & management
- iv) Payments processing
- v) Loans disbursement & management
- vi) Processing cash deposits & withdrawals
- vii) Processing payments & cheques
- viii) Processing & servicing loans
- ix) Accounts management
- x) Configuring & calculating interest
- xi) Customer Relationship Management (CRM) activities
- xii) Setting criteria for minimum balances, interest rates, withdrawals allowed, limits
- xiii) Maintaining records for all bank's transactions

Core features of CBS

- i) On-line real-time processing
- ii) Transactions are posted immediately
- iii) All databases updated simultaneously
- iv) Centralized Operations
- v) Separate hierarchy for business & operations
- vi) Business & Services are productized
- vii) Remote interaction with customers
- viii) Reliance on transaction balancing
- ix) Authorizations occur within application
- x) Increased access by staff at various levels based on authorization
- xi) Daily, half yearly & annual closing
- xii) Automatic processing of standing instructions
- xiii) Centralized interest applications for all accounts & account types
- xiv) Anytime, anywhere access to customers & vendors

Technology Components

- i) Database Environment
- ii) Application Environment
- iii) Web Environment
- iv) Security solution
- v) Connectivity to Corporate Network &
- vi) Data Centre & Disaster Recovery Centre
- vii) Network Solution architecture to provide total connectivity
- viii) Enterprise Security architecture
- ix) Branch & Delivery channel environment
- x) Online Transaction monitoring for fraud risk management

How Does CBS Work?

- i) Planning
- ii) Approval
- iii) Selection
- iv) Design & develop or procured
- v) Testing
- vi) Implementation
- vii) Maintenance
- viii) Support
- ix) Updation
- x) Audit

CBS IT Environment

Types of servers used in deploying CBS.

- i) Application Server
- ii) Database Server
- iii) Automated Teller Machines (ATM) Channel Server
- iv) Internet Banking Channel Server (IBCS)
- v) Internet Banking Application Server
- vi) Web Server
- vii) Proxy Server
- viii) Anti-Virus Software Server

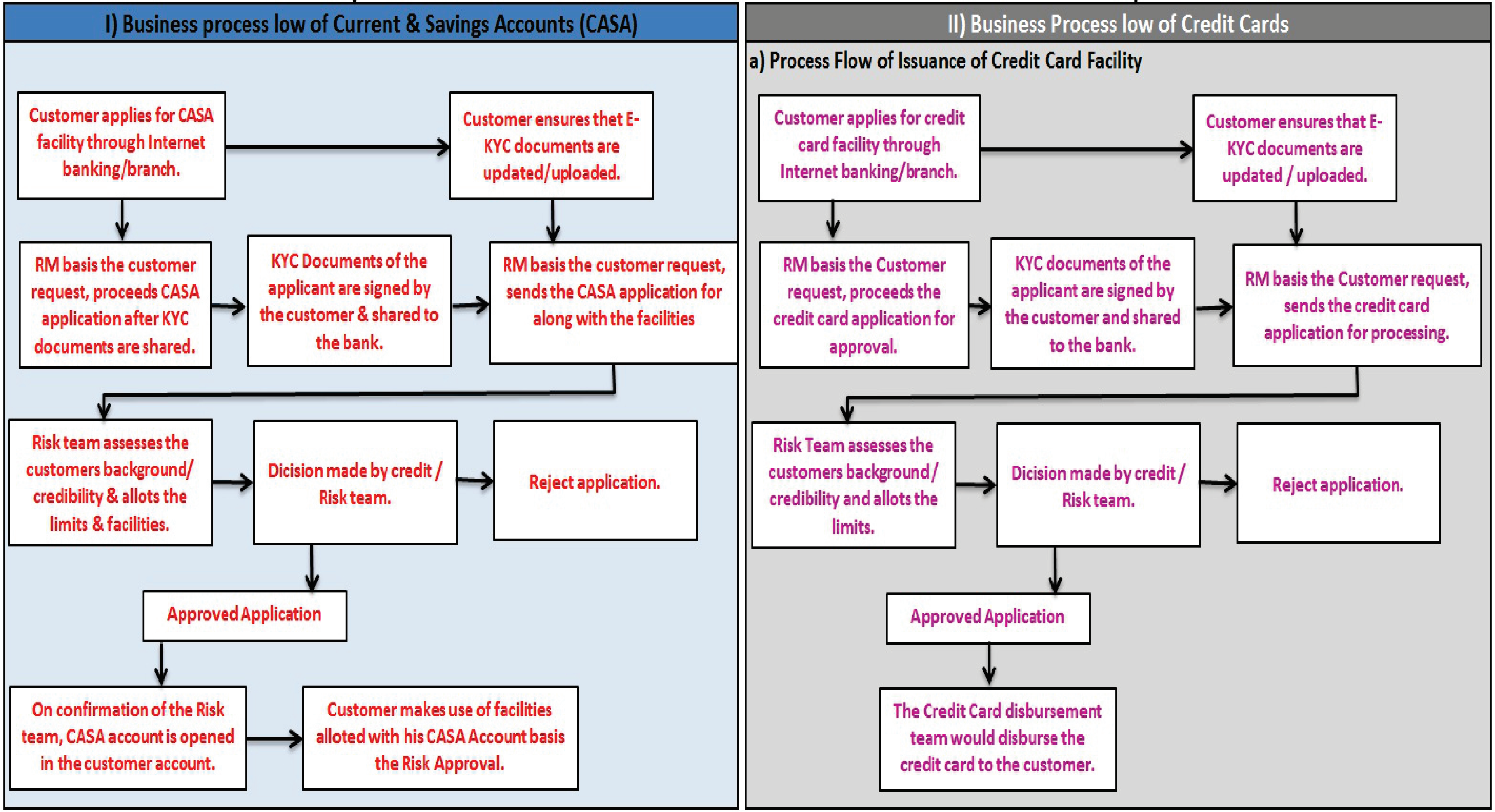
SP CLASSES For CA -CPT, IPCC & FINAL Since 2010 your Success Point

Designed By: **Swapnil Patni**
- CA, CS, LLB, B.Com., CISA
- Expertise knowledge in ISCA, IT, SM, LAW
- Presence all over India at the age of 29
- Also known as the "Motivational Guru"

Team SPC

CORE BANKING SYSTEMS (Chart 5.55)

Core Business Flow & Relevant Risks and Controls



I) Business process low of Current & Savings Accounts (CASA)

Customer applies for CASA facility through Internet banking/branch.

Customer ensures thet E-KYC documents are updated/uploaded.

RM basis the customer request, proceeds CASA application after KYC documents are shared.

KYC Documents of the applicant are signed by the customer & shared to the bank.

RM basis the customer request, sends the CASA application for along with the facilities

Risk team assesses the customers background/ credibility & allots the limits & facilities.

Dicision made by credit / Risk team.

Reject application.

Approved Application

On confirmation of the Risk team, CASA account is opened in the customer account.

Customer makes use of facilities alloted with his CASA Account basis the Risk Approval.

II) Business Process low of Credit Cards

a) Process Flow of Issuance of Credit Card Facility

Customer applies for credit card facility through Internet banking/branch.

Customer ensures that E-KYC documents are updated / uploaded.

RM basis the Customer request, proceeds the credit card application for approval.

KYC documents of the applicant are signed by the customer and shared to the bank.

RM basis the Customer request, sends the credit card application for processing.

Risk Team assesses the customers background / credibility and allots the limits.

Dicision made by credit / Risk team.

Reject application.

Approved Application

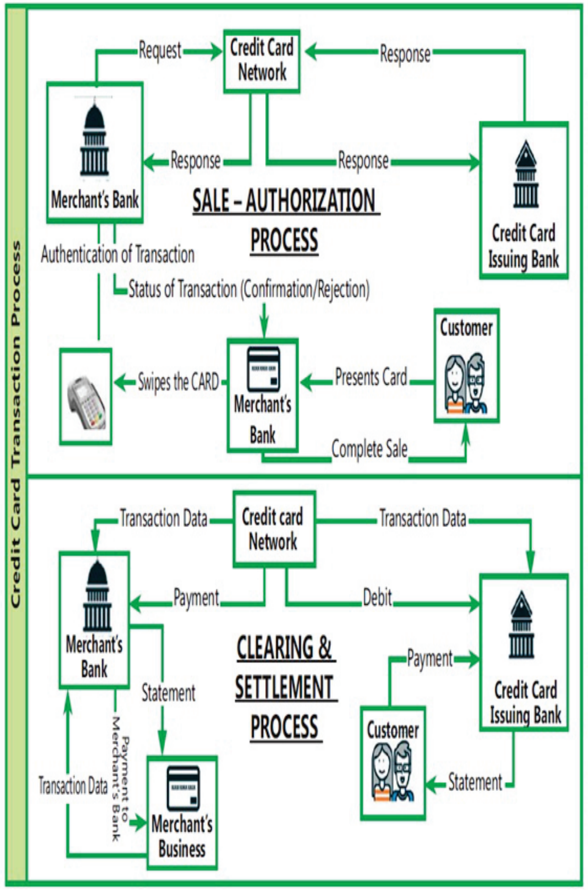
The Credit Card disbursement team would disburse the credit card to the customer.

CORE BANKING SYSTEMS (Chart 5.56)

Core Business Flow & Relevant Risks and Controls

II) Business Process low of Credit Cards

b) Process Flow of Sale - Authorization process of Credit Card Facility



III) Business Process Flow of Mortgages

i) Types of Mortgage Loan

a) Home loan

b) Top up loan

c) Loans for Under Construction Property

ii) Process Description

a) Loans are provided by lender which is a financial institution. There are 2 types of loan widely offered to customer first is fixed rate mortgage second is variable/ floating rate mortgage.

b) Borrower/Customer approaches bank for a mortgage & relationship manager/ loan officer explains customer about home loan . Customer to fill loan application & provide requisite KYC documents.

c) Loan officer reviews loan application & sends it to Credit risk team who will calculate financial obligation income ratio . along with customer documents details are sent to underwriting team for approval.

d) Underwriter will ensure that loan provided is within lending guidelines & at this stage provide conditional approval along with list of documents required

e) As per property selected by customer, loan officer will provide property details along with requisite documents to the legal & valuation team.

f) Further verification of property to determine whether property is built as per approved plan, builder has received requisite certificates, age of building to determine whether it will withstand loan tenure, construction quality

g) Legal & valuation team will send their report to operations team, which entails all details of loan

h) Customer will agree to loan agreement which is offered by signing offer letter. Loan officer will notarize all loan documents & are send back to lender operations team

i) Once signed offer letter is received operations team release or disburse fund & prepare a cashier order

j) Post disbursement of loan customer can carry out various loan servicing activity by visiting the branch or via online mode amendments

IV) Treasury Process

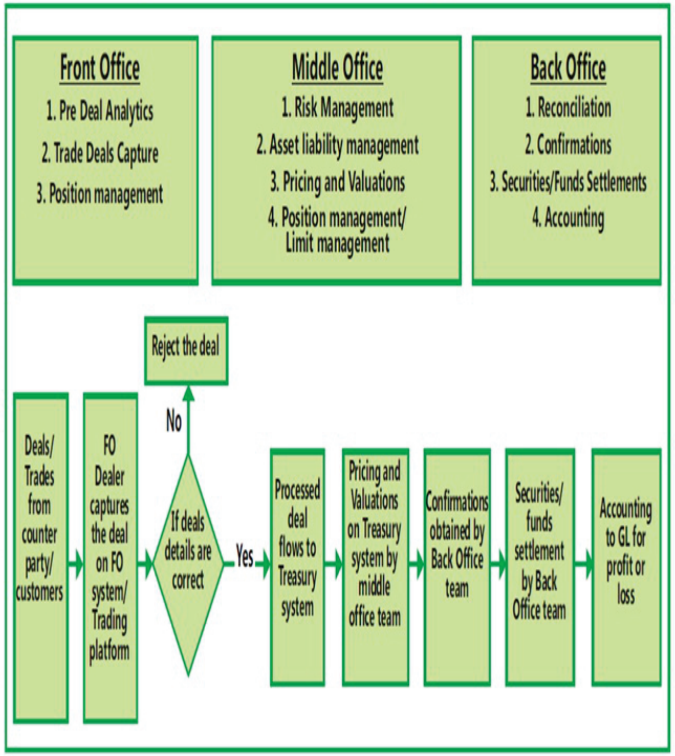
i) Core areas of Treasury Operations

a) Dealing Room Operations (Front office operations)

b) Middle Office (Market Risk department / Product Control Group)

c) Back office.

ii) Process flow for Bank Treasury Operations



Front Office
1. Pre Deal Analytics
2. Trade Deals Capture
3. Position management

Middle Office
1. Risk Management
2. Asset liability management
3. Pricing and Valuations
4. Position management/ Limit management

Back Office
1. Reconciliation
2. Confirmations
3. Securities/Funds Settlements
4. Accounting

Deals/ Trades from counter party/ customers
FO Dealer captures the deal on FO system/ Trading platform
If deals details are correct
No
Reject the deal
Yes
Processed deal flows to Treasury system
Pricing and Valuations on Treasury system by middle office team
Confirmations obtained by Back Office team
Securities/ funds settlement by Back Office team
Accounting to GL for profit or loss

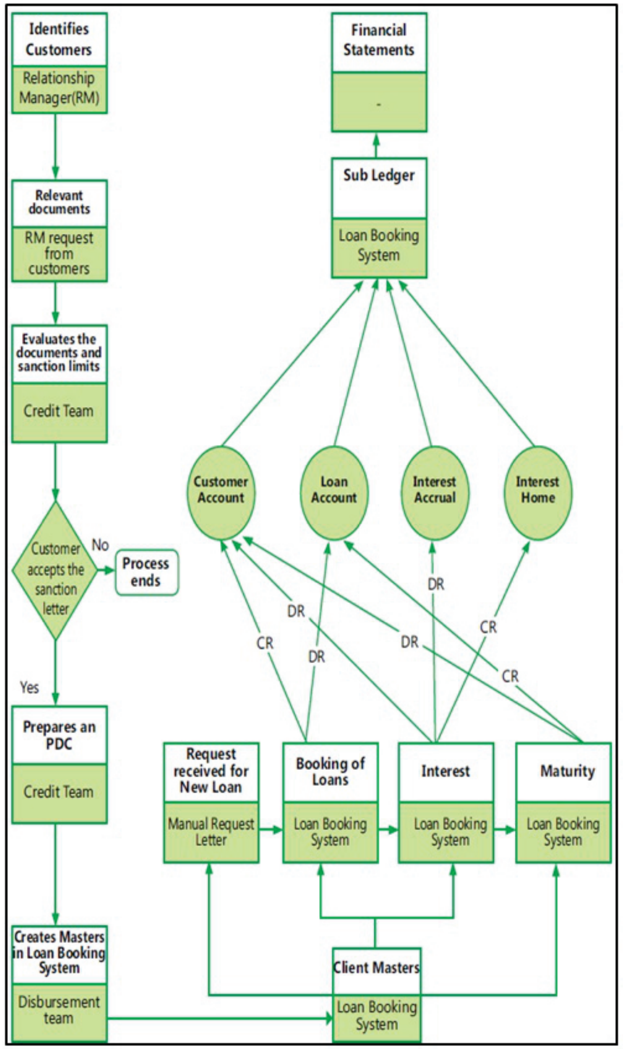
CORE BANKING SYSTEMS (Chart 5.57)

Core Business Flow & Relevant Risks and Controls

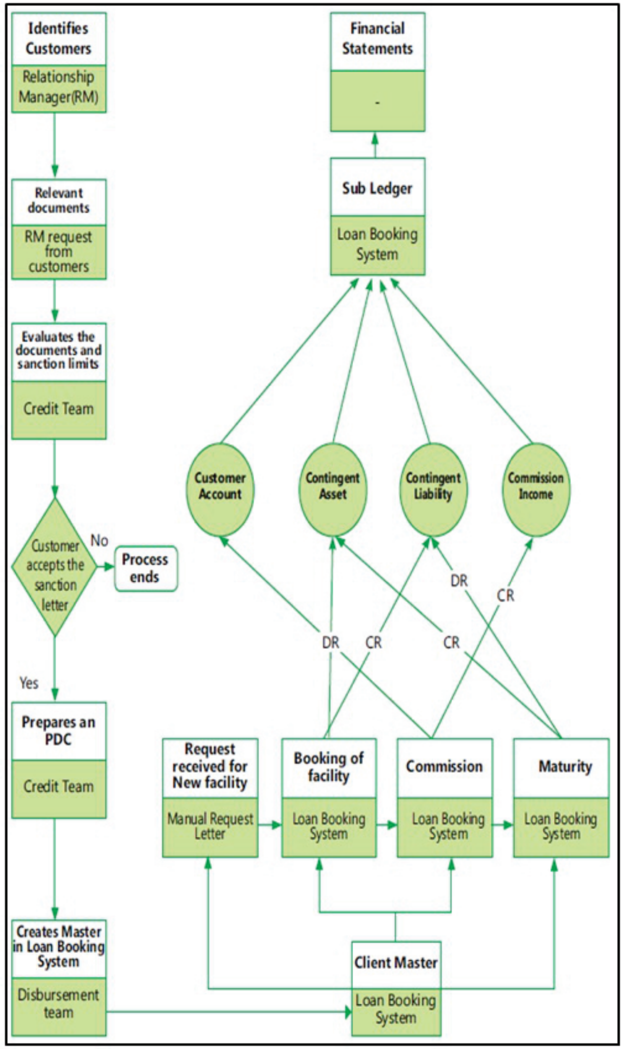
V) Loans & Trade Finance Process

Classification of Credit Facilities:

a) Fund Based Credit Facilities



b) Non-Fund Based Credit Facilities



VI) Internet Banking Process

Customer is provided internet banking facility, which would include:

a) Password change

b) Balance inquiry

c) Fund transfer

d) Request for cheque book

e) Stop payment

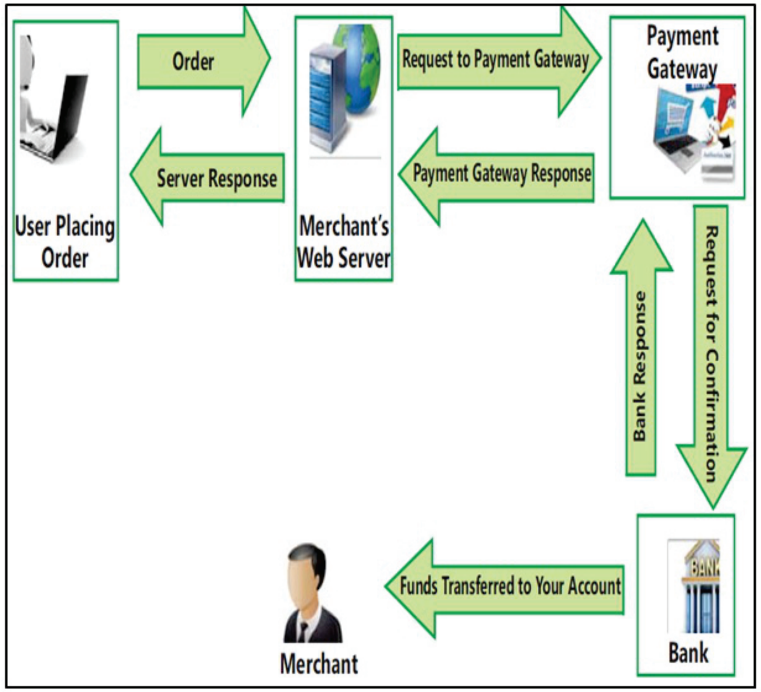
f) Copy of statement of account

g) ATM/ Credit Card related queries

VII) E-Commerce Transaction processing

a) Most of e-Commerce transactions involve advance payment either through a credit or debit card issued by a bank

b) flow of transaction when a customer buys online from vendor's e-commerce website.:-



CORE BANKING SYSTEMS (Chart 5.58)

Core Business Flow & Relevant Risks and Controls

VIII) Risks associated with CBS

a) Ownership of Data/ process

b) Authorization process

c) Authentication procedures

d) Several software interfaces across diverse networks

e) Maintaining response time

f) User Identity Management

g) Access Controls

h) Incident handling procedures

i) Change Management

IX) IT related Risks and mitigating Controls

a) Classification of Risk:-

i) Efficiency	v) Integrity
ii) Effectiveness	vi) Availability
iii) Reliability	vii) Compliance
iv) Confidentiality	

b) Data Centre & Network Operations

i) Backups & Restoring of data

ii) Job & Batch Scheduling and Processing

iii) Monitoring of Applications & supporting Servers

iv) Value Add areas of Service Level Agreements (SLA)

v) User training & qualification of Operations personnel

c) Information Security

i) Information Security Policies, Procedures, & practices

ii) User Security Administration

iii) Application Security

iv) Database Security

v) Operating System Security

vi) Network Security

vii) Physical Security

d) Application Software

Functions of the software are:-

i) Configuration	iii) Transactions
ii) Masters	iv) Reports

Applicable Regulatory & Compliance Requirement

I) Banking Regulation Act

Act provides a framework using which commercial banking in India is supervised & regulated

II) Negotiable Instruments Act-1881 (NI Act)

a) Under NI Act, Cheque includes electronic image of truncated cheque & a cheque in electronic form.

b) A cheque in the electronic form has been defined as 'a mirror image' of a paper cheque

III) RBI Regulations

Some of the key functions of RBI:-

a) Monetary Authority

b) Regulator & supervisor of financial system:

c) Issuer of currency

IV) Information Technology Act

a) Cyber crimes

b) Computer related offences

Examples of offences in IT Act-

i) Section 65: Tampering with Computer Source Documents

ii) Section 66: Computer Related Offences

iii) Section 66-B: Punishment for dishonestly receiving stolen computer resource or communication device

v) Section 66-D: Punishment for cheating by personation by using computer resource

vi) Section 66-E: Punishment for violation of privacy

IV) Money Laundering

It is process by which proceeds of crime & true ownership of those proceeds are concealed or made opaque so that proceeds appear to come from a legitimate source

a) Prevention of Money Laundering Act (PMLA)

- key aspects of PMLA

i) Maintenance of record of all cash transactions above Rs. 10L

ii) All series of cash transactions of value less than Rs. 10 lakhs integrally connected if they have taken place within a month

iii) All cash transactions here forged or counterfeit notes have been used

iv) All suspicious transactions made in cash or otherwise

- 3 stages of Money Laundering

i) Placement

ii) Layering

iii) Integration

- Anti-Money laundering (AML) using Technology

- Financing of Terrorism

VI) Sensitive Personal Data Information (SPDI)

CORE BANKING SYSTEMS (Chart 5.59)

I) Risk around CASA Process

a) Credit Line setup is unauthorized & not in line with banks policy.

b) Customer Master defined in CBS is not in accordance with Pre- Disbursement Certificate.

c) Inaccurate interest / charge being calculated in CBS.

d) Unauthorized personnel approving CA-SAS transaction in CBS.

e) Inaccurate accounting entries generated in CBS.

II) Risks around Credit Card Process

a) Credit Line setup is unauthorized & not in line with banks policy

b) Credit Line setup is unauthorized & not in line with banks policy.

c) Masters defined for customer are not in accordance with Pre-Disbursement Certificate.

d) Credit Line setup can be breached.

e) Inaccurate interest / charge being calculated in Credit Card system.

f) Inaccurate reconciliations performed.

III) Risk around Mortgage Process

a) Incorrect customer & loan details are captured which will affect overall downstream process.

b) Incorrect loan amount disbursed.

c) Interest amount is incorrectly calculated & charged.

d) Unauthorized changes made to loan master data or customer data.

IV) Risk around Treasury Process

a) Unauthorized securities setup in systems such as Front office/Back office

b) Inaccurate trade is processed.

c) Unauthorized confirmations are processed.

d) Insufficient Securities available for Settlement

e) Incomplete & inaccurate data flow between systems.

f) Insufficien funds are available for settlements.

g) Incorrect Nostro payments processed.

V) Risk in Loans & Advances Process

a) Credit Line setup is unauthorized & not in line with banks policy.

b) Credit Line setup is unauthorized & not in line with banks policy.

c) Masters defined for customer are not in accordance with Pre-Disbursement Certificate.

d) Credit Line setup can be breached in Loan disbursement system/CBS.

e) Lower rate of interest/ Comm may be charged to customer.

f) Facilities/Loan's granted may be unauthorized/inappropriate

g) Inaccurate interest / charge being calculated in Loan disbursal system

VI) Risks w.r.t Data Centre & Network Operations

a) Transaction may not be recorded completely or accurately, & related items will be inaccurately or incompletely recorded.

b) Invalid items may be recorded or valid items may be inaccurately or incompletely recorded.

c) Timely & adequate technical support may not be available & issues may not be resolved.

d) User queries may not be timely & adequately resolved.

e) Timely execution & complete processing & availability of data may not be ensured

f) Unavailability of applications & data backups in event of a disaster. It can also result in disclosure of sensitive info

g) Data may be lost & systems may not be recoverable in event of a serious system failure. This may result in regulatory/ legal complaints, loss of reputation beside financial loss.

h) Backup may not be available

VII) Risks & Controls w.r.t Information Security

a) Significant information resources may be modified inappropriately, disclosed without authorization, and/ or unavailable when needed.

b) Lack of management direction & commitment to protect information assets.

c) User accountability is not established.

d) Unauthorized system or data access, loss & modification due to virus

d) Potential Loss of confidenti-ality, availability & integrity of data & system.

e) It is easier for unauthorized users to guess password of an authorized user & access system and/ or data. This may result in loss of confidentiality, availability & integrity of data & system.

f) Unauthorized viewing, modification or copying of data and/ or unauthorized use, modification or denial of service in system.

g) Potential loss of confidentiality, availability & integrity of data & system

h) Inadequate preventive measure for key server & IT system in case of environmental threat like heat, humidity, fire, flood etc.

d) Security breaches may go undetected.

VIII) Risks w.r.t Application Controls

a) Interest may be incorrectly computed leading to incorrect recording of income/ expenditure.

b) Inappropriate assignment of rate codes resulting in violation of business rules &/ or loss of revenue.

c) Absence of appropriate system validations may result in violation of business rules.

d) Inappropriate reversal of charges resulting in loss of revenue.

e) Failure to levy appropriate charges resulting in loss of revenue.

f) Multiple liens in excess of deposit value may result in inability recover outstanding in event of a default.

g) Inappropriate security or controls over system parameter settings resulting in unauthorized or incorrect changes to settings.

h) Inappropriate set up of accounts resulting in violation of business rules

i) Failure to automate closure of NRE/ NRO accounts on change in residence status may result in regulatory non-compliance & undue benefits to customers.

j) Failure to levy appropriate charges resulting in loss of revenue. Inappropriate levy of charges, resulting in customer disputes.

k) Incorrect classification and provisioning of NPAs, resulting in financial misstatement.