

AUTOMATED BUSINESS PROCESS (Chart 1.37)

Categories of Business Processes

Operational Processes	Supporting Processes	Management Processes
Order to Cash Cycle (Eg)- It is a set of business processes that involves receiving & fulfilling customer requests for goods or services	Human Resource Management (Eg.)- Main HR Process Areas are grouped into logical functional areas & they are as follows-	Budgeting (Eg.)- Having a formal & structured budgeting process is foundation for good business management, growth & development
An order to cash cycle consists of multiple sub-processes:-	i) Recruitment & Staffing ii) Goal Setting iii) Training & Development iv) Compensation & Benefits v) Performance Management vi) Leadership Development vii) Career 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 specific function & can be implemented for many different functions of company activities. BPA is tactic a business uses to automate processes to operate efficiently & effectively. BPA is tradition of analyzing, documenting, optimizing & then automating business processes.

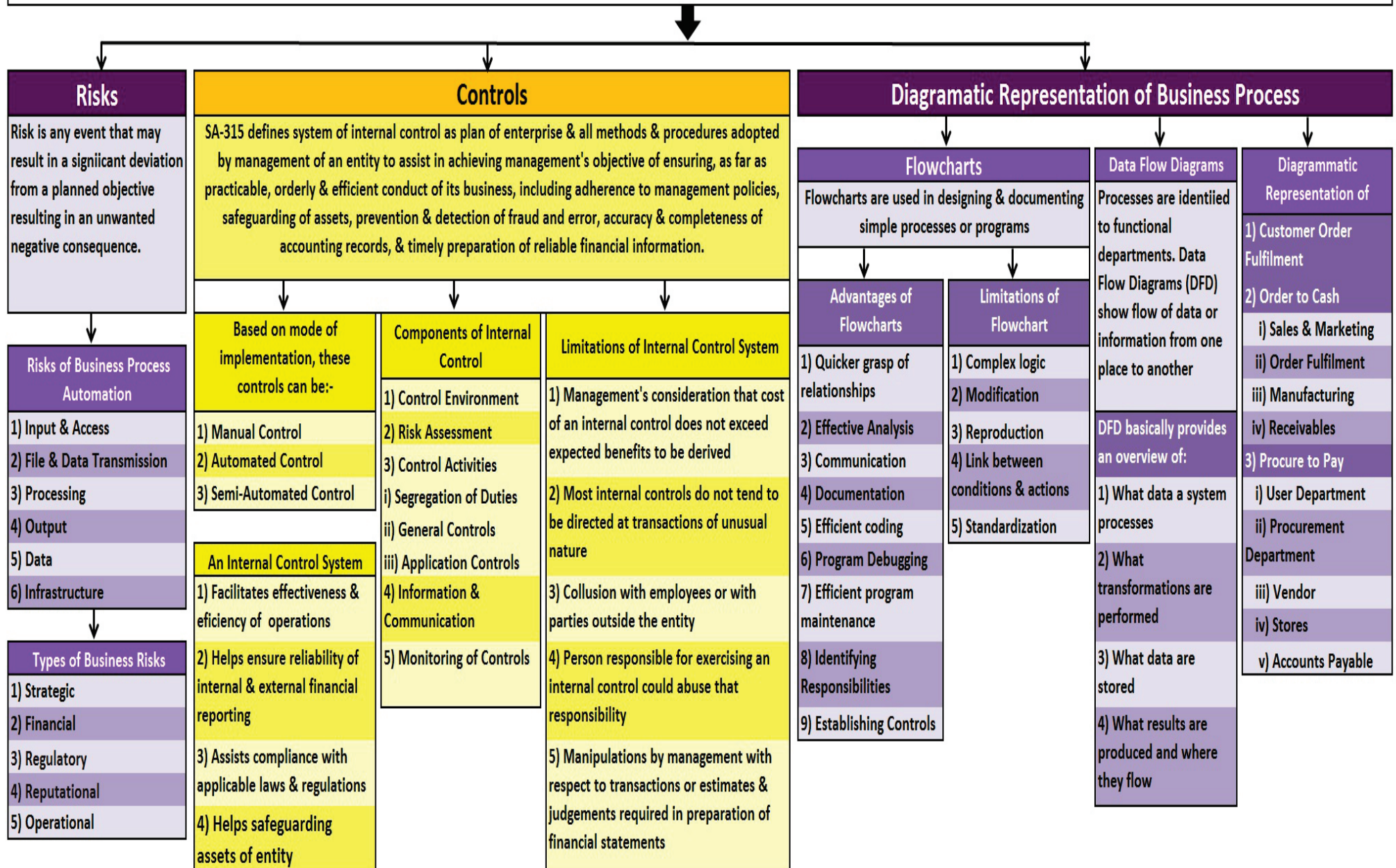
Objectives of BPA	Implementation of BPA
1) Confidentiality 2) Integrity 3) Availability 4) Timeliness	1) Step 1: Define why we plan to implement a BPA? 2) Step 2: Understand rules / regulation under which enterprise needs to comply with? 3) Step 3: Document process, we wish to automate 4) Step 4: Define 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
Benefits	
1) Quality & Consistency 2) Time Saving 3) Visibility 4) Improved Operational Efficiency 5) Governance & Reliability 6) Reduced Turnaround Times 7) Reduced Costs	

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 2) Link growth, risk and return 3) Enhance risk response decisions 4) Minimize operational surprises & losses	5) Identify & manage cross-enterprise risks 6) Provide integrated responses to multiple risks 7) Seize opportunities 8) Rationalize capital
Components of Enterprise Risk Management	
1) Internal Environment 2) Objective Setting 3) Event Identification 4) Risk Assessment	5) Risk Response 6) Control Activities 7) Information & Communication 8) Monitoring

AUTOMATED BUSINESS PROCESS (Chart 1.38)



AUTOMATED BUSINESS PROCESS (Chart 1.39)

Risks And Controls For Specific Business Process

Business Processes - Risks & Controls	Procure to Pay – Risks & Controls	Order to Cash (O2C) – Risks & Controls	Inventory Cycle – Risks & Controls	Human Resources – Risks & Controls	General Ledger – Risks & Controls	Fixed Assets – Risks & Controls
Suitable controls should be implemented to meet requirements of control objectives.	It is process of obtaining & managing raw materials needed for manufacturing a product or providing a service	It is a set of business processes that involve receiving & fulfilling customer requests for goods or services	It is a process of accurately tracking on-hand inventory levels for an enterprise	Stage of HR cycle includes following:	Steps in general ledger process flow are as follows:	Steps of fixed assets process are as follows:
Levels of Computer controls:		It consists of multiple sub-processes including:	Phases of Inventory Cycle for Manufacturers:	1) Recruiting & On boarding	1) Entering inancial transactions into system	1) Procuring an asset
1) Configuration		1) Customer order is documented	1) The ordering phase	2) Orientation & Career Planning	2) Reviewing Transactions	2) Registering or Adding an asset
2) Masters		2) Order is fulfilled or service is scheduled	2) The production phase	3) Career Development	3) Approving Transactions	3) Adjusting the Assets
3) Transactions		3) Order is shipped to customer or service is performed	3) The finished goods & delivery phase	4) Termination or Transition	4) Posting of Transactions	4) Transferring the Assets
		4) Invoice is created & sent to customer			5) Generating Financial	5) Depreciating the Assets
		5) Customer sends payment /Collection				6) Disposing the Assets
		6) Payment is recorded in general				



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)

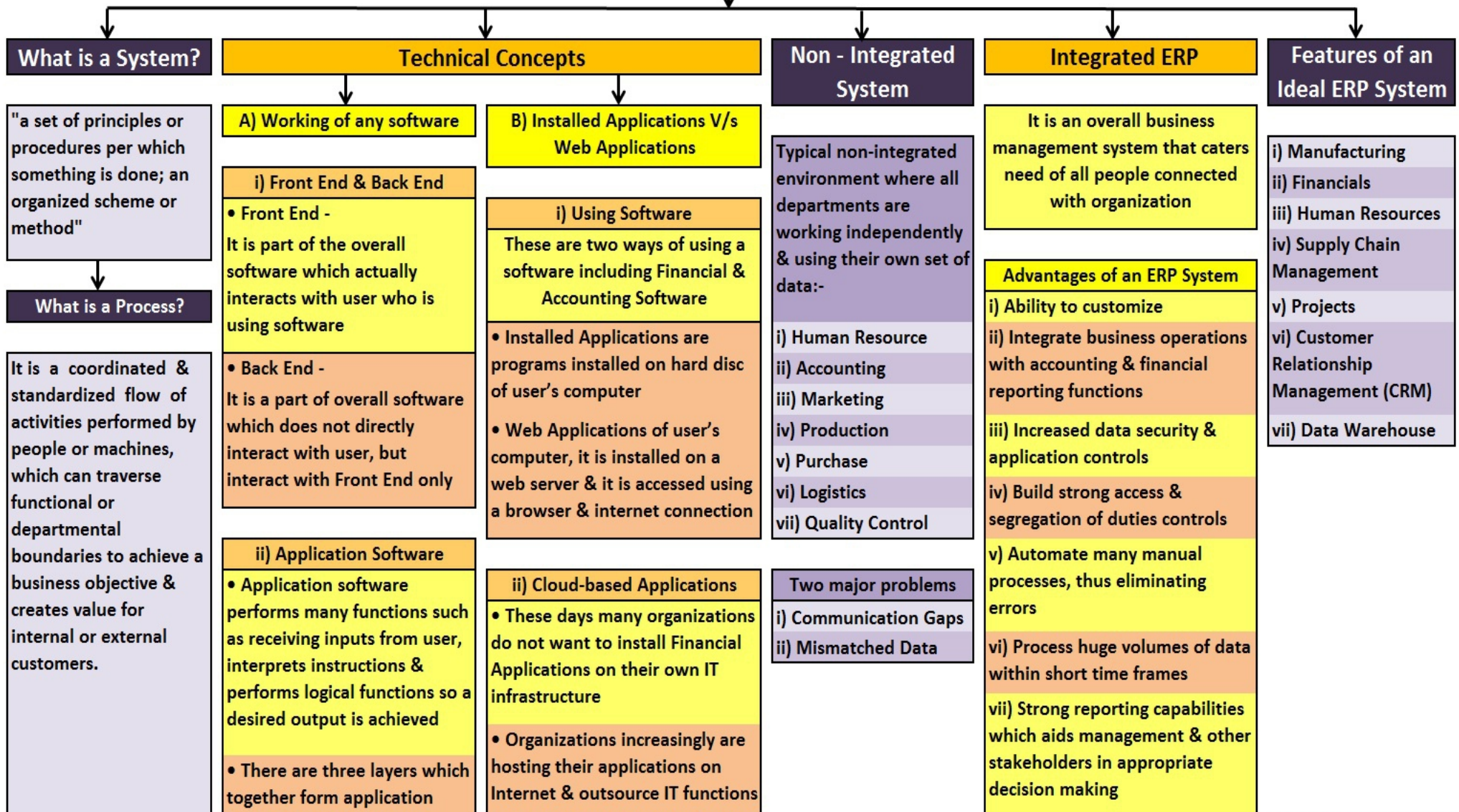
a) Rule 3 defines sensitive personal information as:

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



FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.39)

Integrated and Non- Integrated Systems

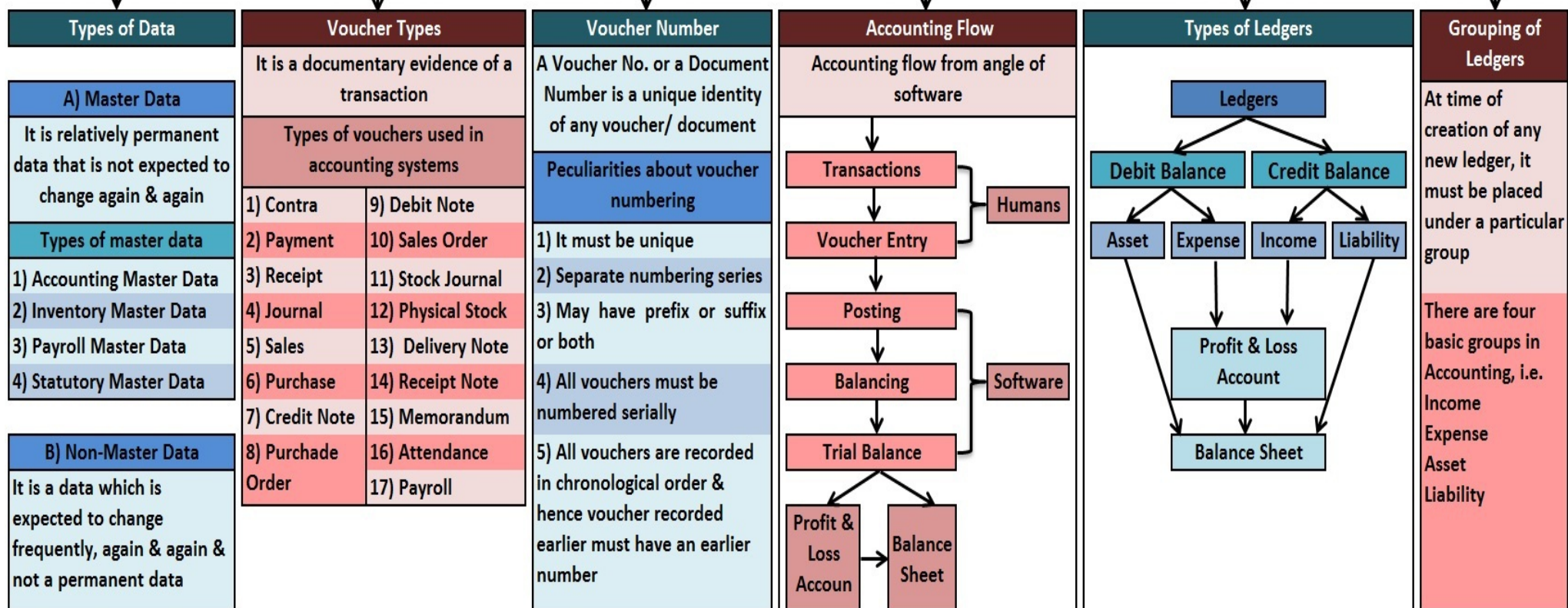


(Continue on Chart 2.40)

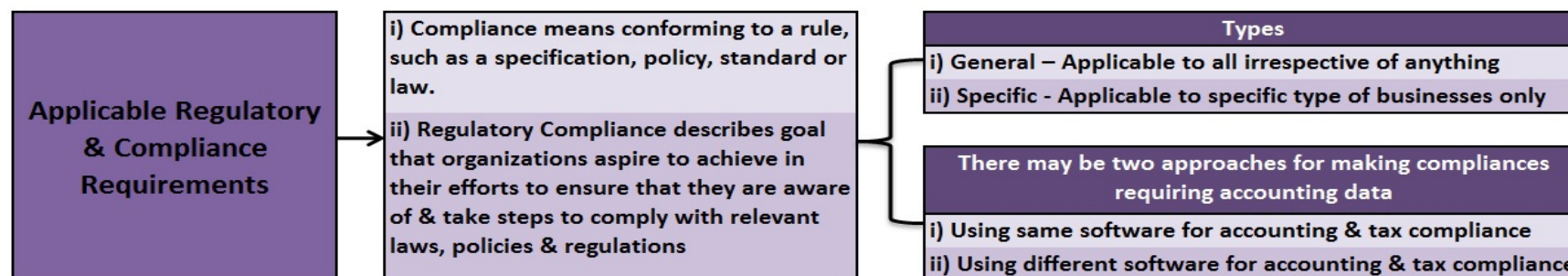
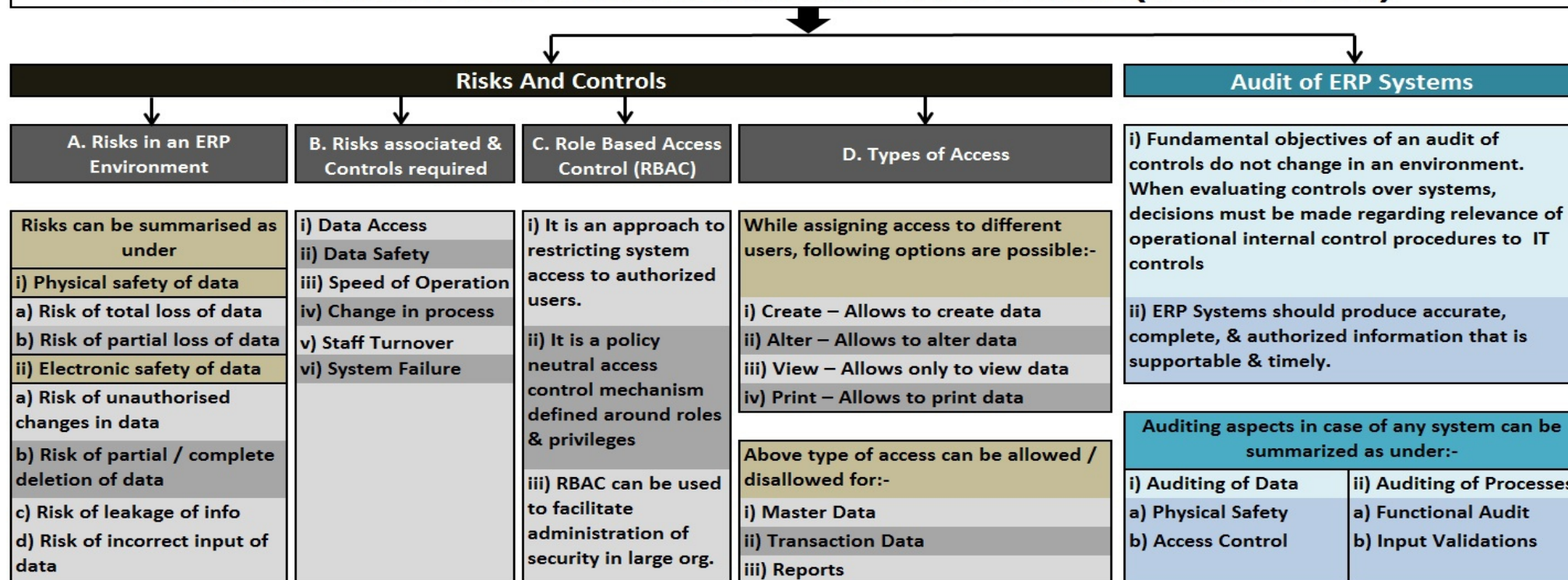
FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.40)

Integrated and Non- Integrated Systems

Concepts in Computerized Accounting Systems



FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.41)



FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.42)

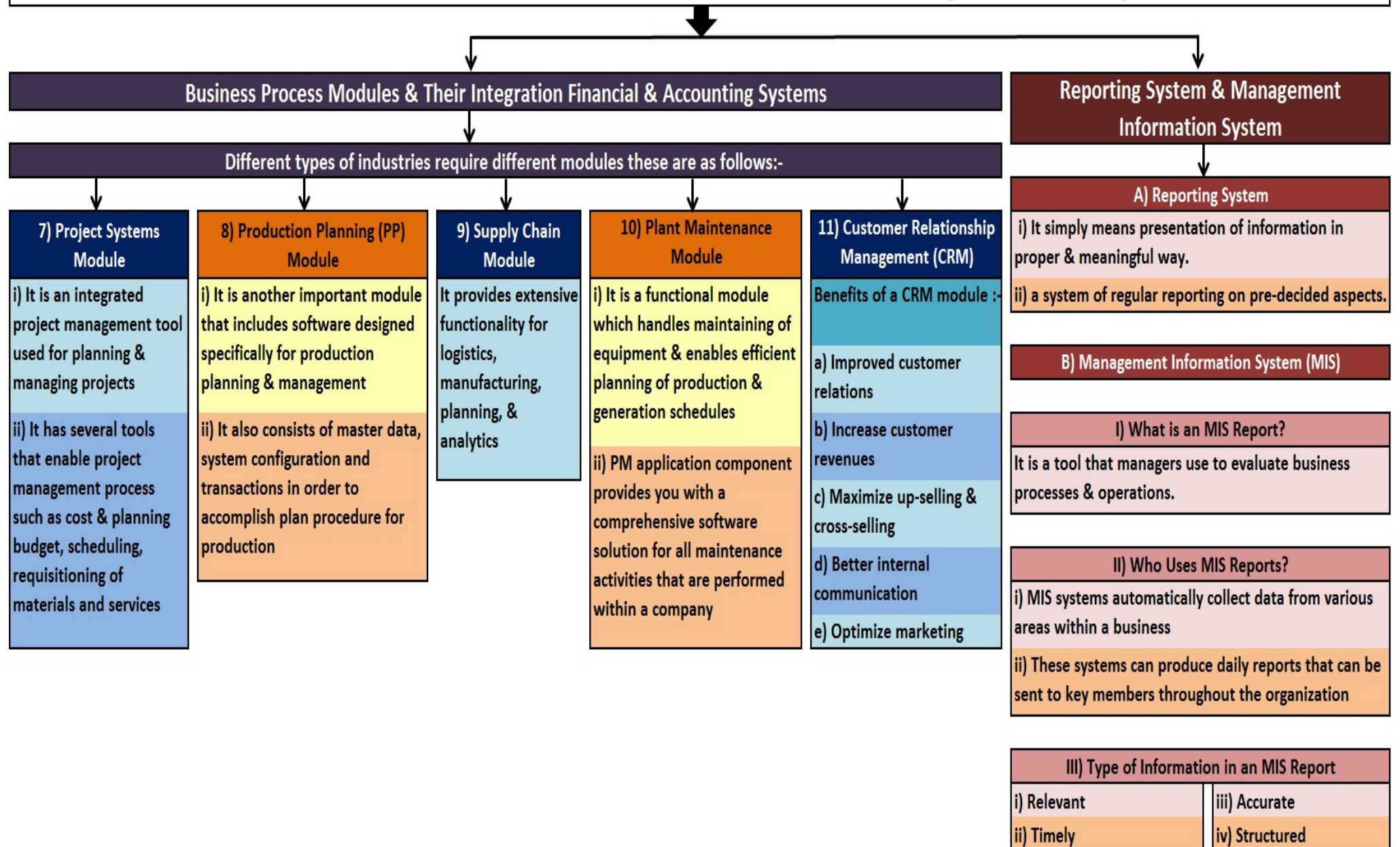
Business Process Modules & Their Integration Financial & Accounting Systems

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

1) Financial Accounting Module	2) Controlling Module	3) Sales & Distribution Module	4) Human Resource Module	5) Quality Management Module	6) Material Management (MM) Module
Features of this module:-	Features of this module:-	Features of this module:-	i) Enhances work process & data management within HR dept of enterprises.	a) Master data & standards are set for quality management	a) Purchase Requisition from Production Dept.
a) Tracking of flow for effective strategic decision making	a) Cost element Accounting	a) Setting up Organization Structure		b) Set Quality Targets to be met	b) Evaluation of Requisition
b) Creation of Organizational Structure	b) Cost Center Accounting	b) Assigning Organizational Units		c) Quality management plan is prepared	c) Asking for Quotation
c) Financial Accounting Global Settings	c) Activity-Based-Accounting	c) Defining pricing Components		d) Define how those quality targets will be measured	d) Evaluation of quotations
d) General ledger Accounting	d) Internal Orders	d) Setting up sales document types, billing types, and tax-related components	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.	e) Take actions needed to measure quality	e) Purchase Order
e) Tax Configuration & Creation & Maintenance of house of Banks	e) Product Cost Controlling	e) Setting up Customer master data records & configuration		f) Identify quality issues & improvements & changes to be made	f) Material Receipt
h) Asset Accounting	f) Profitability Analysis	Sales & Distribution Process		g) Any change is needed in product, change requests are sent	g) Issue of material
f) Account payables	g) Profit Center Accounting	a) Pre - Sales Activities		h) Report on overall level of quality achieved	h) Purchase Invoice
g) Account receivables		b) Sales Order		i) Quality is checked at multiple points	i) Payment to Vendor
i) Integration with Sales & Distribution &		c) Inventory Sourcing			
		d) Material Delivery			
		e) Billing			
		f) Receipt from Customer			

(Continue on Chart 2.43)

FINANCIAL AND ACCOUNTING SYSTEMS (Chart 2.43)



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

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

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

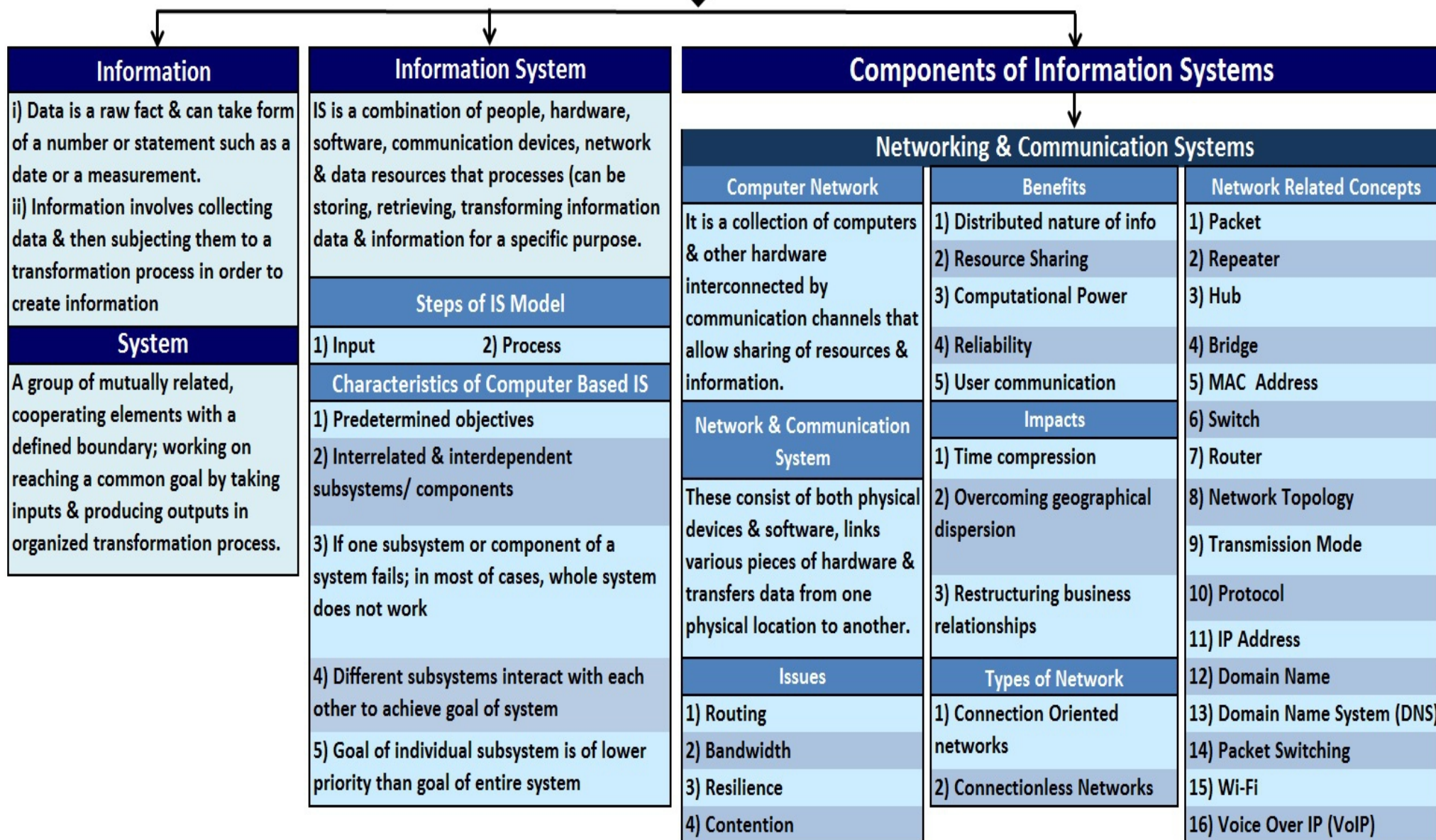
Inside Data Analytics Process

- 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)



(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	Processing Devices	Data Storage Devices	Output Devices
Through which we interact with systems & include devices like Keyboard, Mouse & other pointing devices, Scanners	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	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 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	Application Software	
It is a set of computer programs that manages computer hardware resources & acts as an interface with computer applications programs.	It includes all that computer software that cause a comp. to perform useful tasks beyond running of comp. itself	
Activities are executed by OS	Types	Benefits
1) Performing hardware functions	1) Application Suite	1) Addressing User needs
2) User Interfaces	2) Enterprise Software	2) Less threat from virus
3) Hardware Independence	3) Enterprise Infra. Software	3) Regular updates
4) Memory Management	4) Information Worker Software	Application Areas
5) Task Management	5) Content Access Software	1) Finance & Accounting
6) Networking Capability	6) Educational Software	2) Marketing & Sales
7) Logical Access Security	7) Media Development Software	3) Production or Mfg.
8) File management	Disadvantages	4) Inventory /Stores Mgmt.
	1) Development is costly	5) Human Resource Mgmt
	2) Infection from Malware	

INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.73)

Classification of Information System's Controls

Objective of Controls	Nature of Information System Resources			
1) Preventive Controls These controls prevent errors, omissions, or security incidents from occurring	1) Environmental Controls Controls relating to IT environment Controls for Environmental Exposures	3) Logical Access Controls These are controls relating to logical access to information resources		
2) Detective Controls These controls are designed to detect errors, omissions or malicious acts that occur & report occurrence.	1) Fire Damage 2) Power Spikes 3) Water Damage 4) Pollution Damage & others	Technical Exposures	Some of Logical Access Controls	
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	2) Physical Access Controls This includes abuse of data processing resources Controls for Physical Exposures	1) Data Diddling 2) Bomb 3) Christmas Card 4) Worm 5) Rounding Down 6) Salami Techniques 7) Trap Doors 8) Spoofing	1) User Access Management i) User Registration ii) Privilege management iii) User password management iv) Review of user access rights	6) Operating System Access Control i) Automated terminal identification ii) Terminal log-in procedures iii) Access Token iv) Access Control List v) Discretionary Access Control vi) User identification & 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
3) Corrective Controls It is desirable to correct errors, omissions, or incidents once they have been detected	Controls for Physical Exposures i) Locks on Doors ii) Physical Identification Medium iii) Logging on Facilities iv) Other means of Controlling Physical Access	Asynchronous Attacks 1) Data Leakage 2) Subversive Attacks 3) Wire tapping 4) Piggybacking	2) User Responsibilities i) Password use ii) Unattended user equipment	
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.	a) Video Cameras b) Security Guards c) Controlled Visitor Access d) Bonded Personnel e) Dead Man Doors f) Non-exposure of Sensitive Facilities g) Computer Terminal Locks h) Controlled Single Entry Point i) Alarm System j) Perimeter Fencing k) Control of out of hours of employee-employees l) Secured Report/Document Distribution Cart	Logical Access Violators 1) Hackers 2) Employees 3) IS Personnel 4) Former Employees 5) End Users	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	

(Continue on Chart 3.74)



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) Staffing 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 Specification 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)

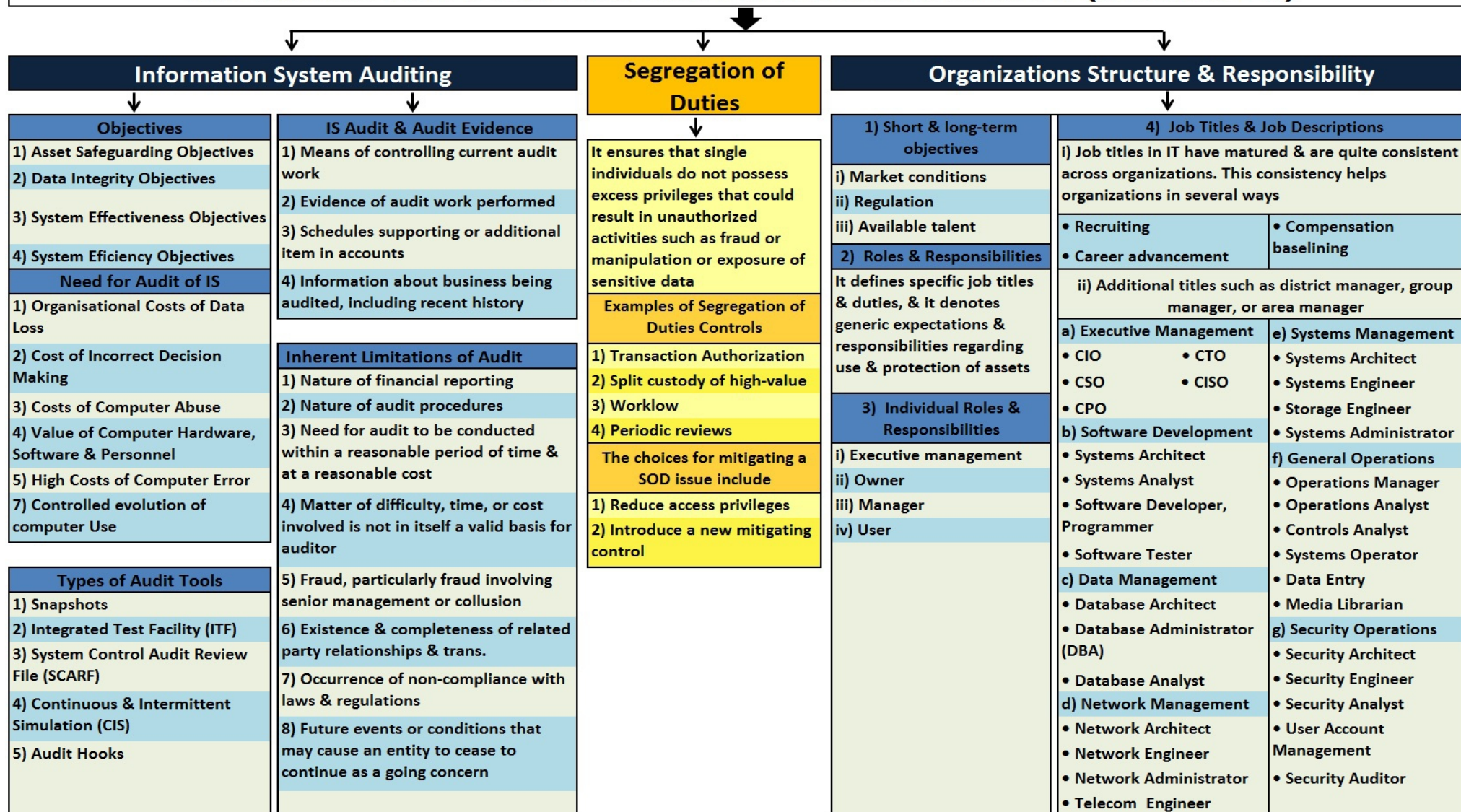
Classification of Information System's Controls

Audit Functions

B) Application Controls & their Categories

I) Boundary Controls	II) Input Controls		III) Communication Controls	IV) Processing Controls	V) Database Controls	VI) Output Controls
a) Major purposes of access control mechanism	a) Source Document Controls	d) Validation Controls	i) Physical Component Controls	i) Processor Controls	i) Major Update Controls	• Storage & Logging of sensitive, critical forms
i) Identification	i) Use pre-numbered source documents	i) Field Interrogation	• Transmission Media	• Error Detection & Correction	• Sequence Check between Transaction & Master Files	• Logging of output program executions
ii) Authentication	ii) Use source documents in sequence	• Limit Check	• Communication Lines	• Multiple Execution States	• Ensure All Records on Files are processed	• Spooling/ Queuing
iii) Authorization	iii) Periodically audit source documents	• Picture Checks	• Modem	• Timing Controls	• Process multiple transactions for a single record in correct order	• Controls over printing
b) Cryptography	b) Data Coding Controls	• Valid Code Checks	• Port Protection Devices	• Component Replication	• Maintain a suspense account	• Report Distribution & Collection Controls
c) Passwords	i) Transcription Errors	• Check Digit	• Multiplexers & Concentrators	ii) Real Memory Controls	ii) Major Report Controls	• Retention Controls
d) Personal Identification Numbers (PIN)	• Addition errors	ii) Record Interrogation	ii) Line Error Control	iii) Virtual Memory Controls	• Standing Data	
e) Identification Cards	• Truncation errors	• Reasonableness Check	• Error Detection	iv) Data Processing Controls	• Print-Run-to Run control Totals	
f) Biometric Devices	• Substitution errors	• Valid Sign	• Error Correction	• Run-to-Run Totals	• Print Suspense Account Entries	
	ii) Transposition Errors	• Sequence Check	iii) Flow Controls	• Reasonableness Verification	• Existence/Recovery Controls	
	• Single transposition	iii) File Interrogation	iv) Link Controls	• Edit Checks		
	• Multiple transposition	• Version Usage	v) Topological Controls	• Field Initialization		
	c) Batch Controls	• Internal & External Labeling	• Local Area Network Topologies	• Exception Reports		
	i) Types of batches	• Data File Security	• Wide Area Network Topologies			
	• Physical Controls	• Before & after Image & Logging	vi) Channel Access Controls			
	• Logical Controls	• File Updating & Maintenance Authorization	• Polling			
	ii) Types of control	• Parity Check	vii) Internetworking Controls			
	• Financial totals					
	• Hash totals					
	• Document/Record Counts					

INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.76)



INFORMATION SYSTEMS AND ITS COMPONENTS (Chart 3.77)

Audit Trail

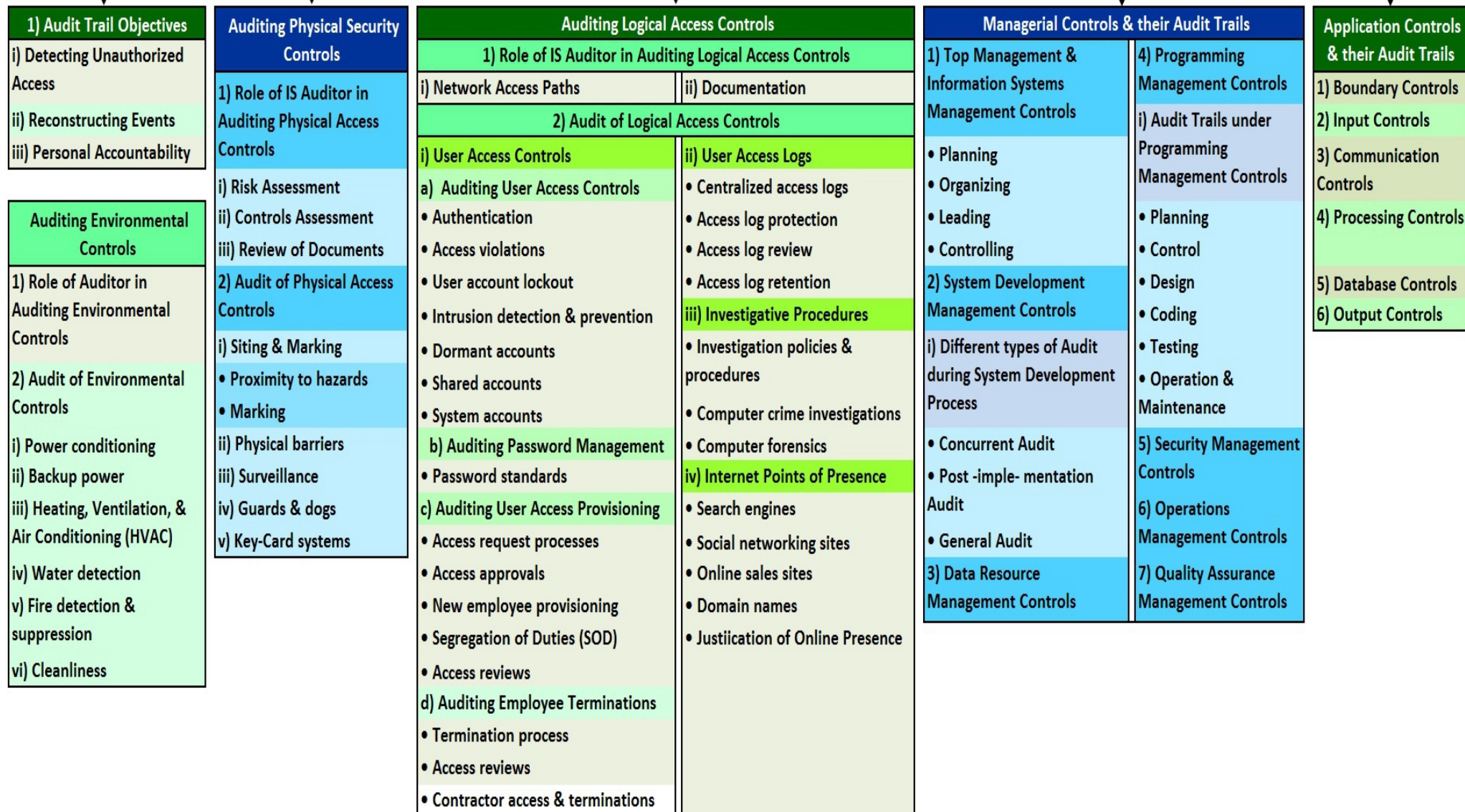
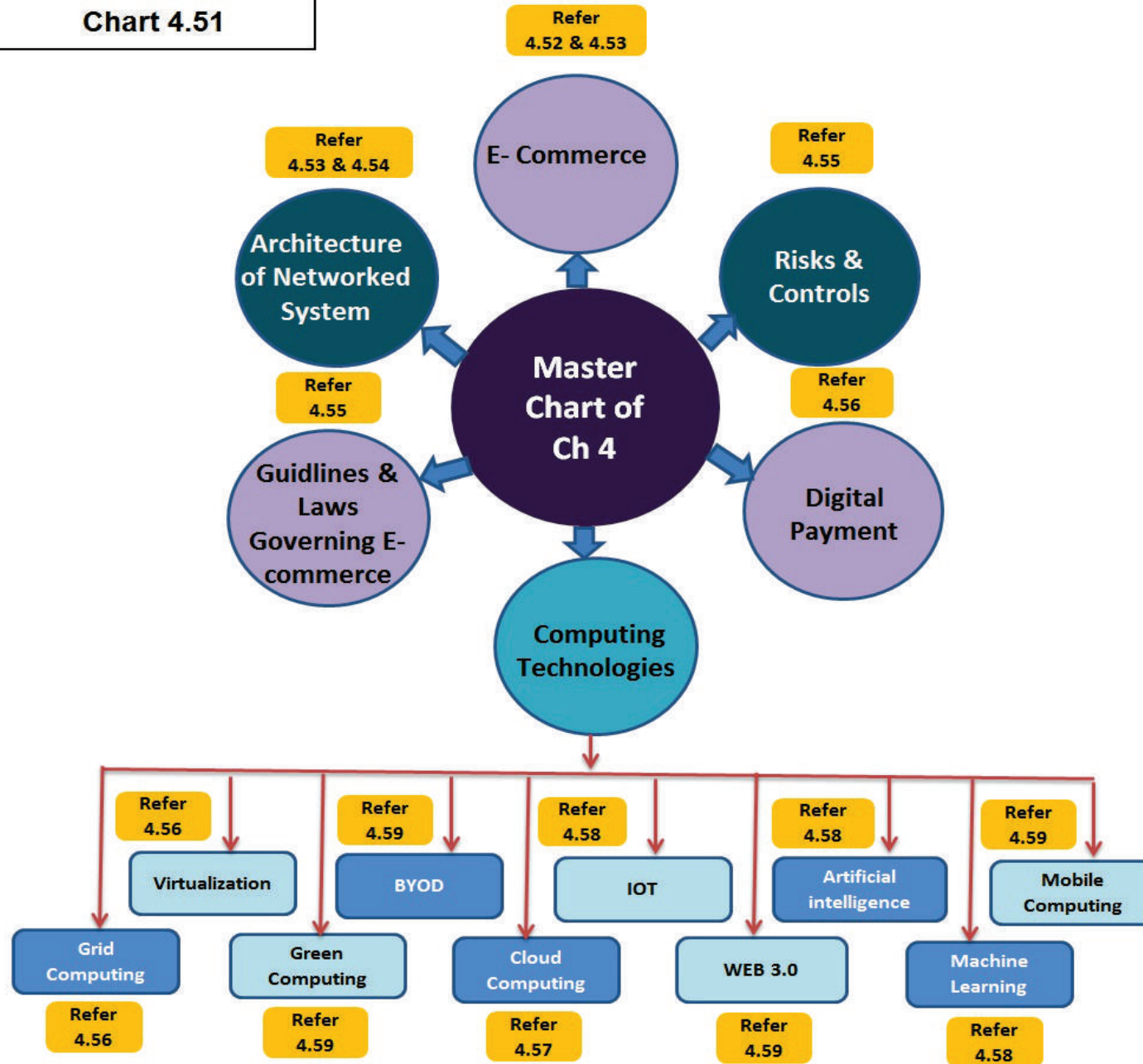


Chart 4.51



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.

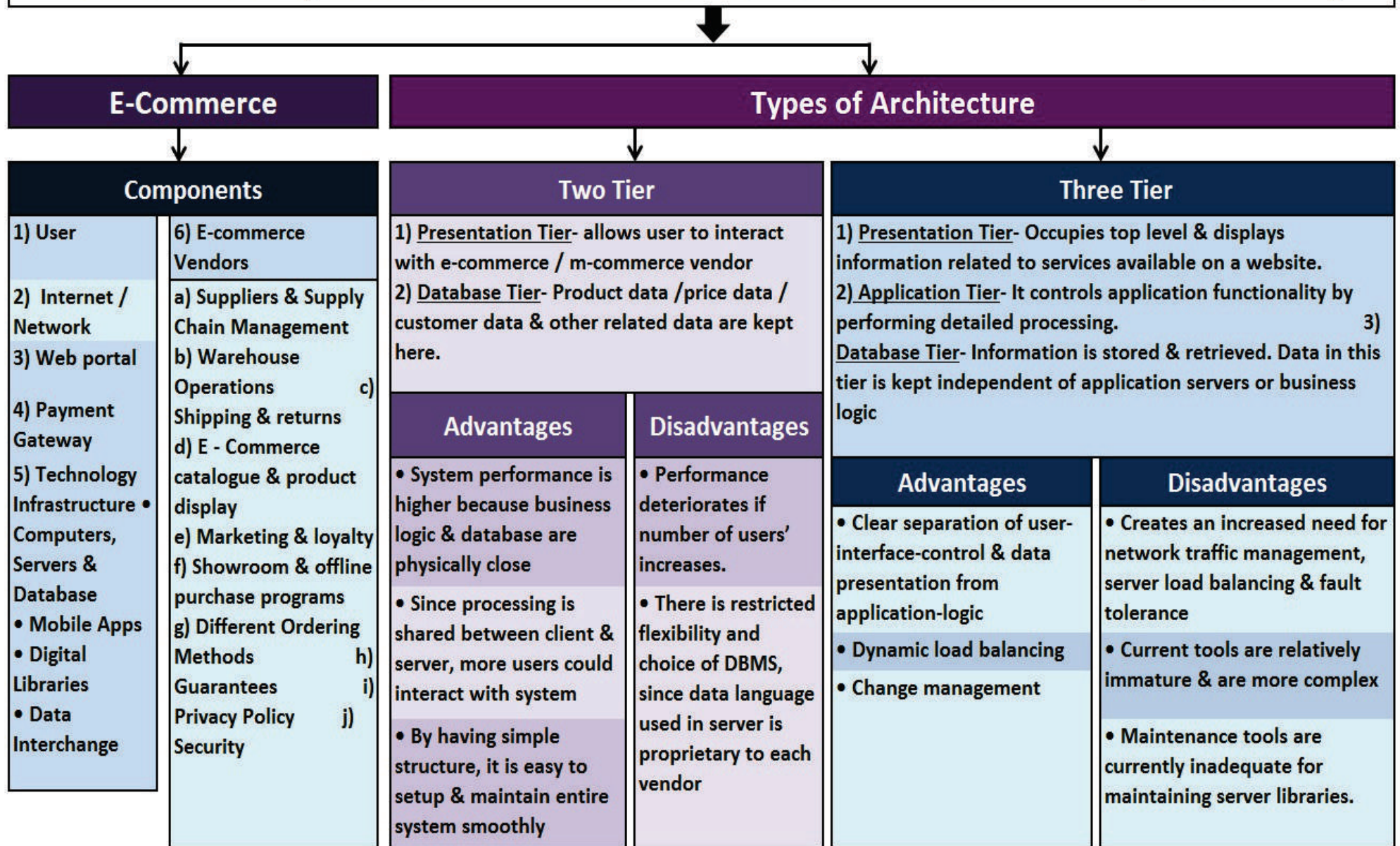
Difference between Traditional commerce & E-Commerce

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 24x7x365
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

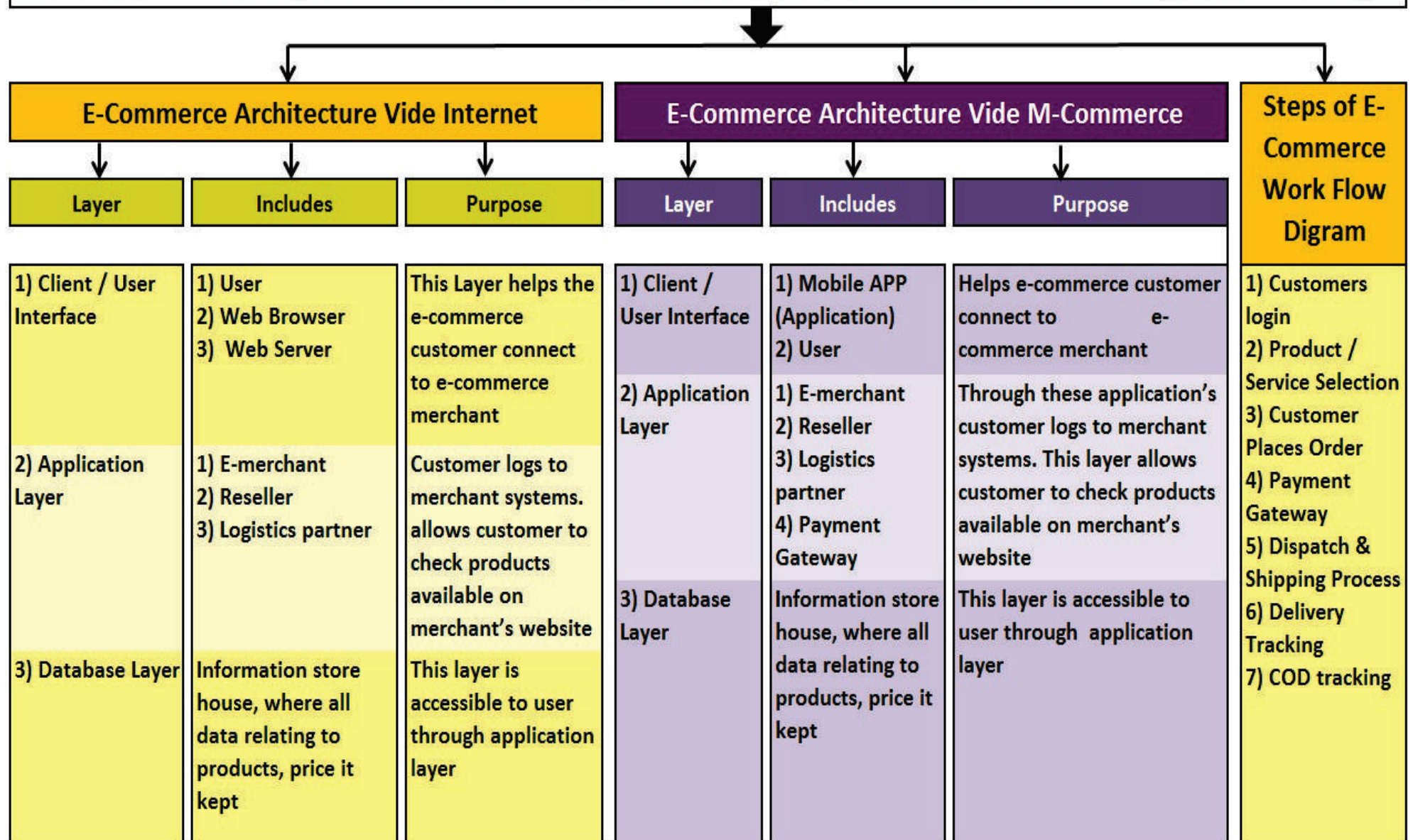
Benefits

To Customer/ Individual/ User	To Business / Sellers	To Government
• Convenience • Time saving • Various Options • Easy to find reviews • Coupon & Deals • Anytime Access	• 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	• Reduction in use of ecologically damaging materials through electronic coordination of activities & movement of information rather than physical objects

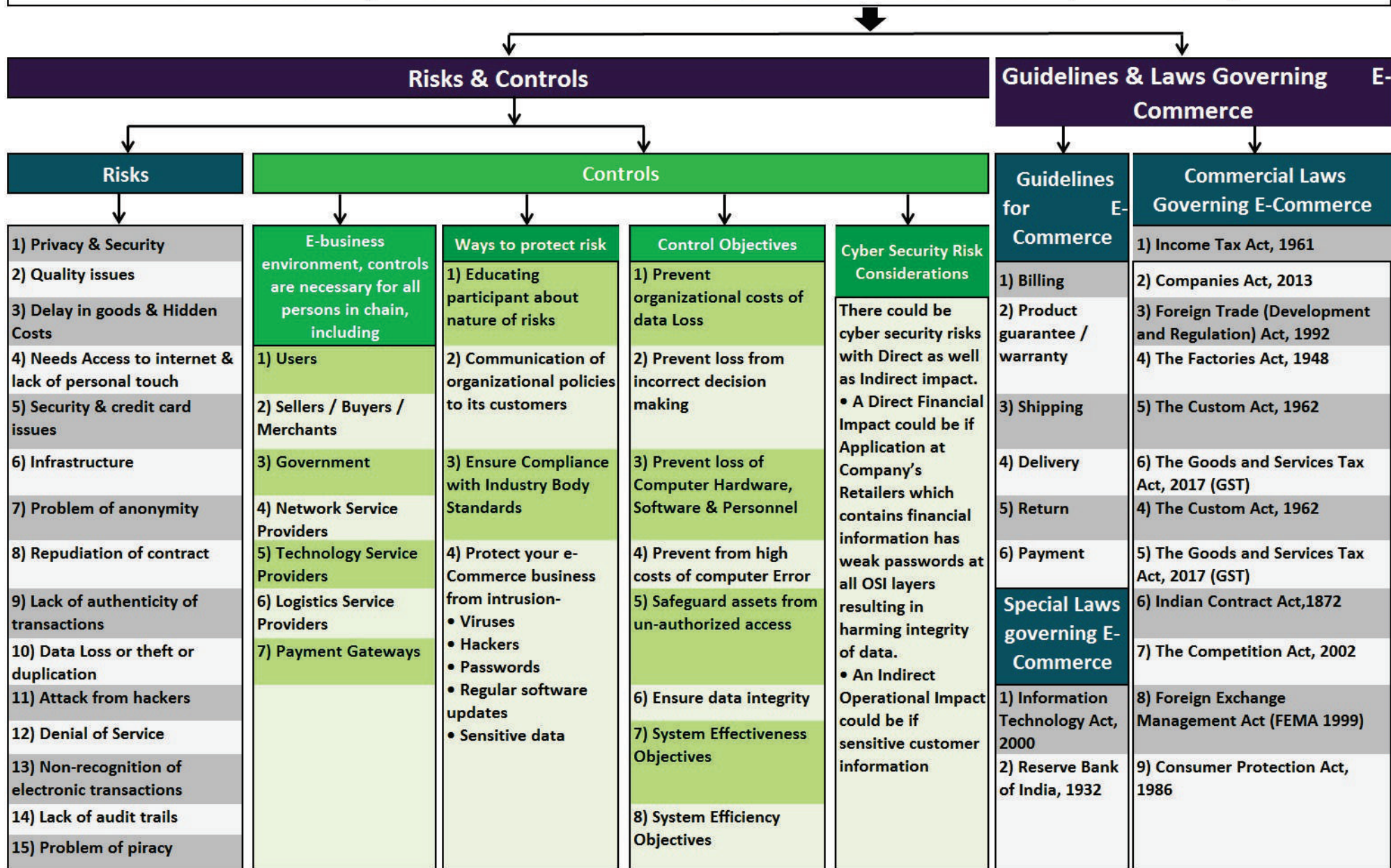
E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.53)



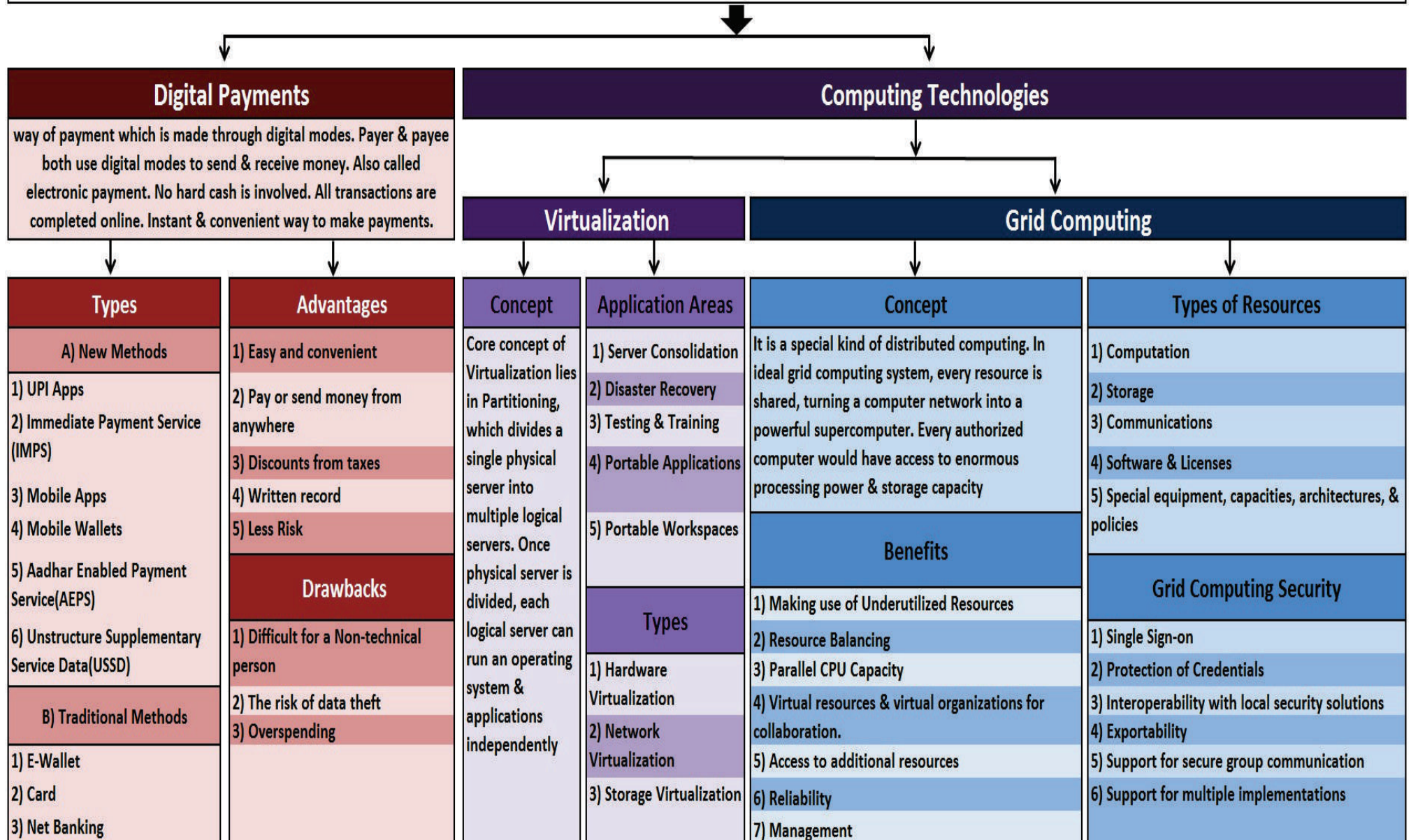
E-COMMERCE, M-COMMERCE AND EMERGING TECHNOLOGY (Chart 4.54)



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



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



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	Public	Hybrid	Community
Resides within boundaries of an organisation & used exclusively for the organisation's benefits	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.	It is a combination of both at least one private (internal) & at least one public (external).	It is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns
Characteristics	Characteristics	Characteristics	Characteristics
1) Secure	1) Highly Scalable	1) Scalable	1) Collaborative & Distributive Maintenance
2) Central Control	2) Affordable	2) Partially Secure	2) Partially Secure
3) Weak Service Level Agreements	3) Less Secure	3) Stringent SLAs	3) Cost Effective
Advantages	Advantages	Advantages	Advantages
1) Improves average server utilization, higher efficiencies in low cost	1) Used in development, deployment & management of enterprise applications, at affordable costs.	4) Complex Cloud Management	1) Establishing a low-cost private cloud
2) High level of security & privacy to user	2) Deliver highly scalable & reliable applications rapidly	Limitation	2) Collaborative work
3) small , controlled & maintained by organization	3) No need for establishing infrastructure for setting up & maintaining cloud	1) Highly scalable	3) Sharing of responsibilities
Limitation	4) Strict SLAs are followed	2) Provides better security than public cloud	4) Better security than public cloud
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	5) There is no limit for number of users	Security features are not as good as private cloud & complex to manage	Limitation
	Limitation		autonomy of organization is lost & some of security features are not.
	Security assurance & thereby building trust among clients is far from desired but slowly liable to happen. Further, privacy & organizational autonomy are not possible		

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

Artificial Intelligence

Definition- 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 | 3) Mobile Software |
| 2) Mobile Hardware | |

Limitations

- | | |
|---------------------------|--------------------------------|
| 1) Insufficient Bandwidth | 4) Transmission interferences |
| 2) Security Standards | 5) Potential health hazards |
| 3) Power consumption | 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	Challenges of IT	IT Risks & Risk Assessment				Applying IT Controls
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	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	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	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	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
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		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			II) Application controls
					VII) Internal Control System in Banks a) Internal Controls in Banks b) IT Controls in Banks	

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

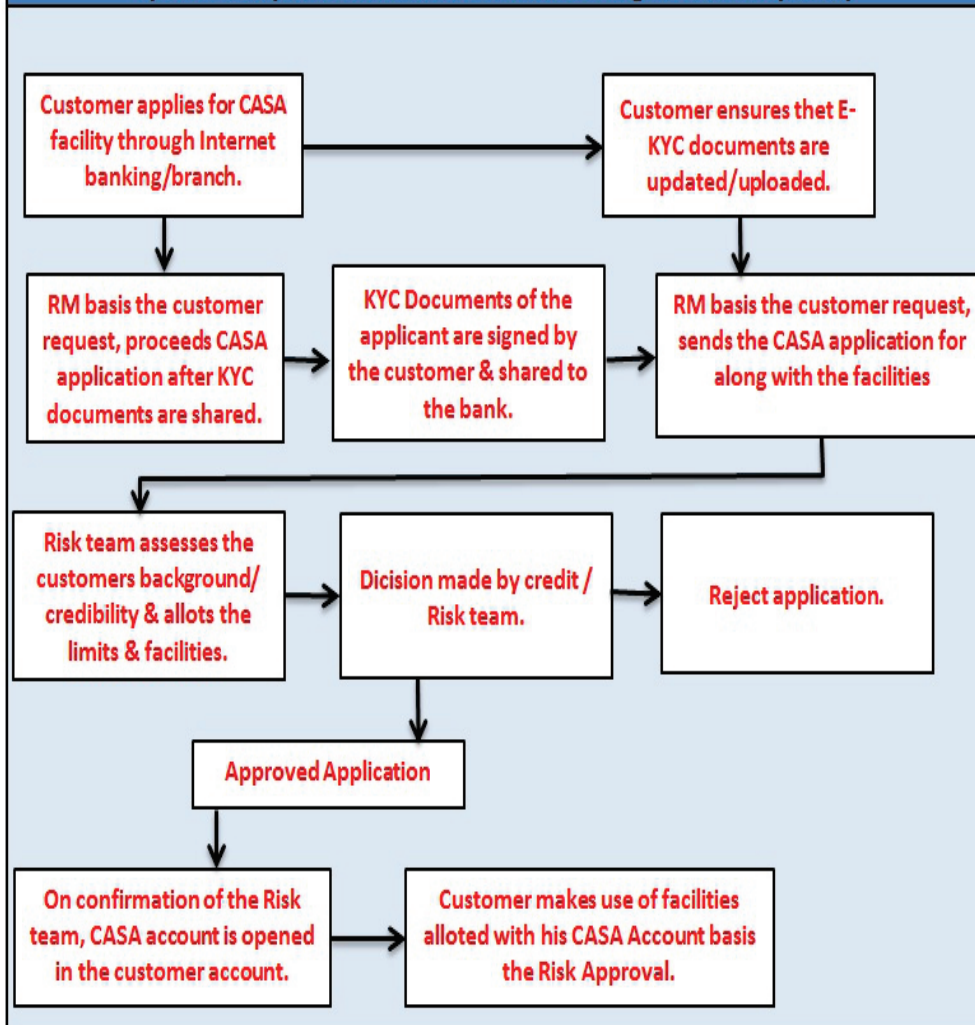
- Types of servers used in deploying CBS.
- i) Application Server
 - ii) Database Server
 - iii) Automated Teller Machines (ATM) Channel Server
 - iv) Internet Banking Channel Server (IBCS)
 - v) Internet Banking Application Server
 - vi) Web Server
 - vii) Proxy Server
 - viii) Anti-Virus Software Server



CORE BANKING SYSTEMS (Chart 5.55)

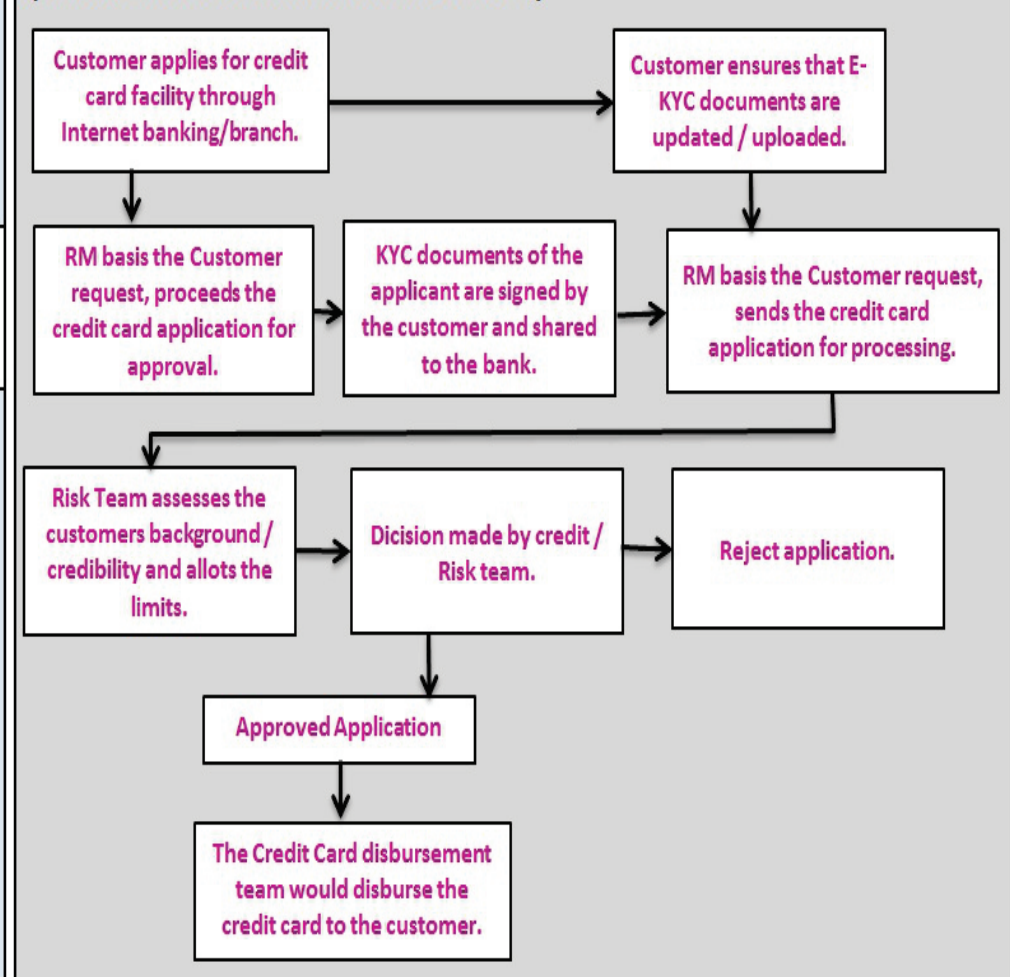
Core Business Flow & Relevant Risks and Controls

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



II) Business Process flow of Credit Cards

a) Process Flow of Issuance of Credit Card Facility

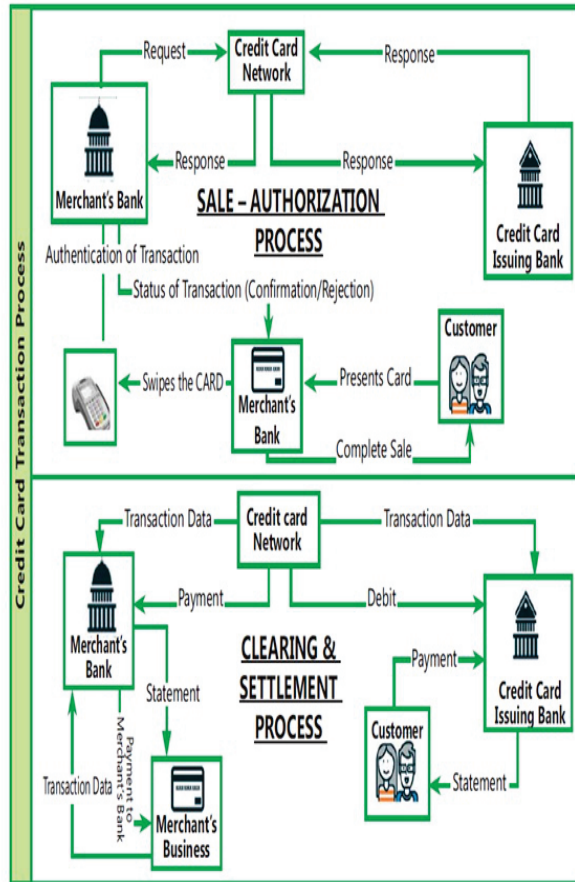


CORE BANKING SYSTEMS (Chart 5.56)

Core Business Flow & Relevant Risks and Controls

II) Business Process flow 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

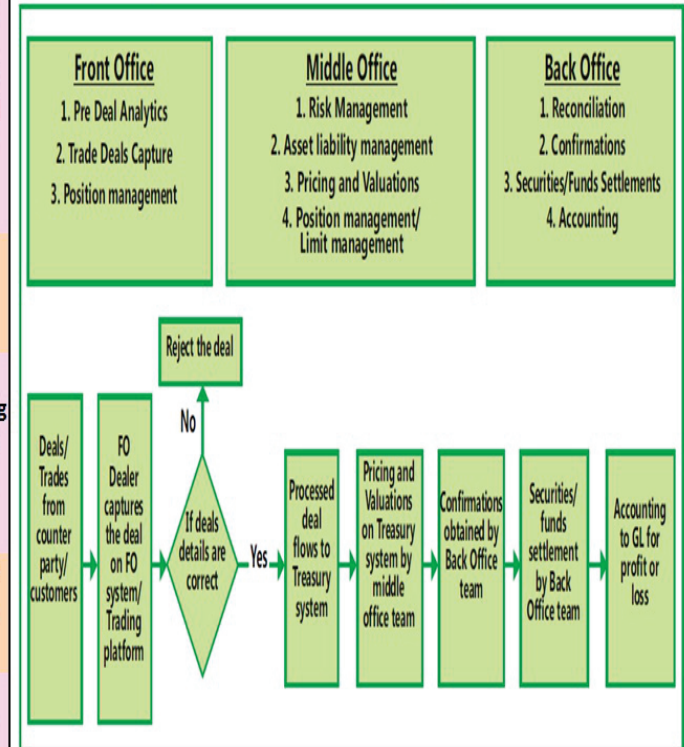
- a) Loans are provided by lender which is a financial institution. There are 2 types of loan widely offered to customer first is fixed rate mortgage second is variable/ floating rate mortgage.
- b) Borrower/Customer approaches bank for a mortgage & relationship manager/ loan officer explains customer 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



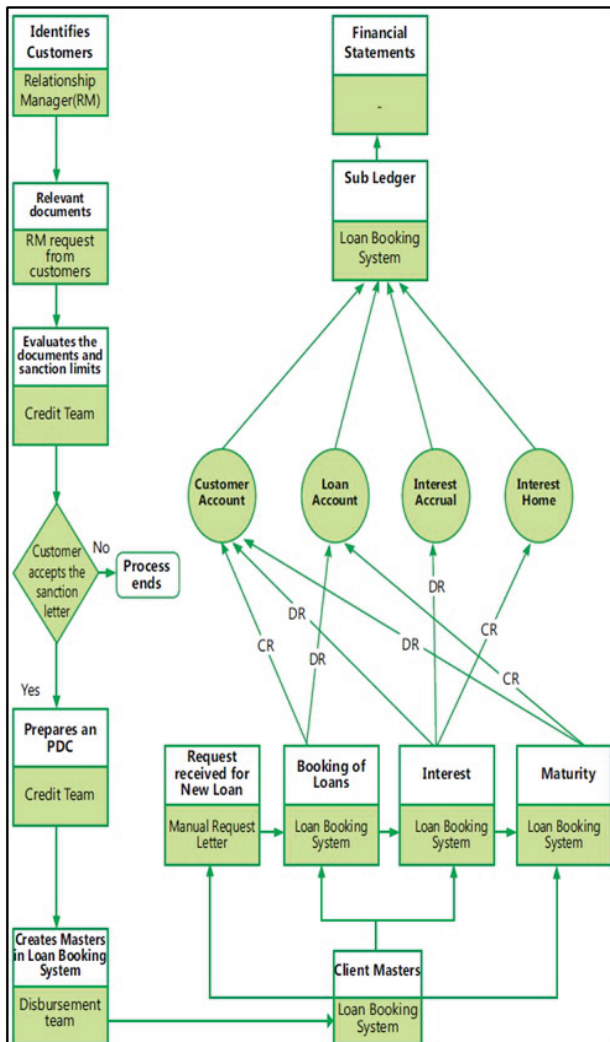
CORE BANKING SYSTEMS (Chart 5.57)

Core Business Flow & Relevant Risks and Controls

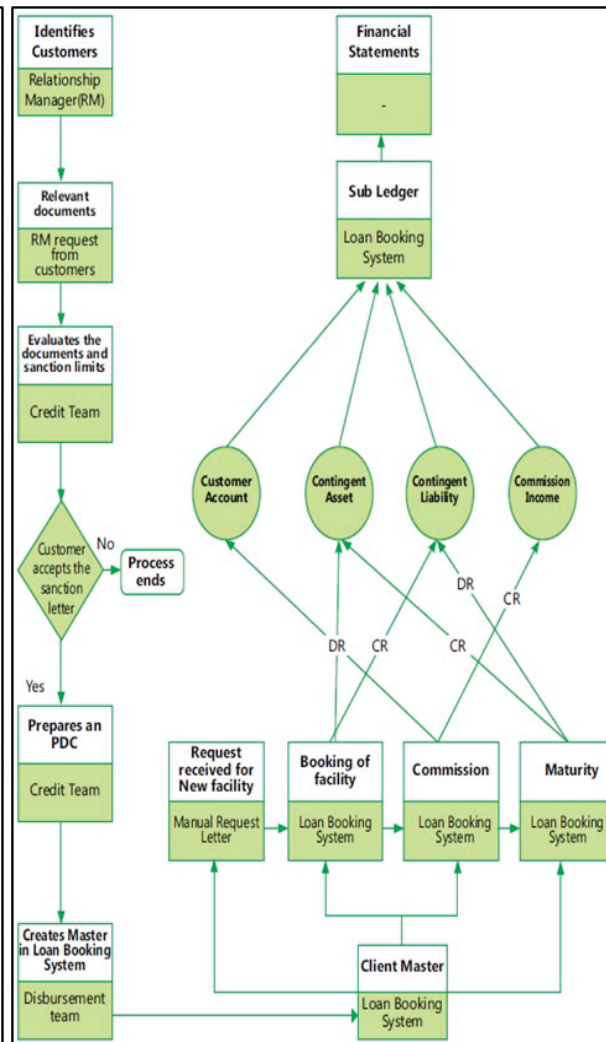
V) Loans & Trade Finance Process

Classification of Credit Facilities:

a) Fund Based Credit Facilities



b) Non-Fund Based Credit Facilities



VI) Internet Banking Process

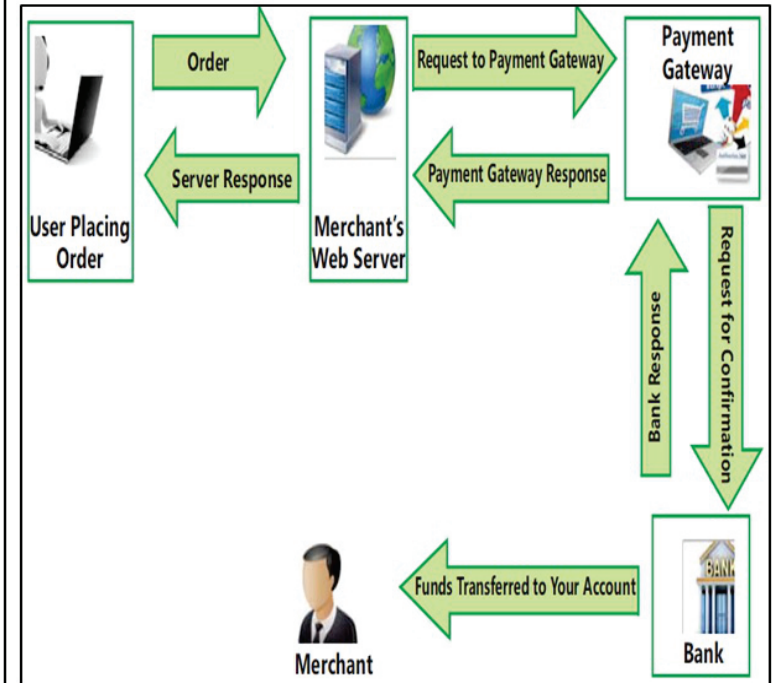
Customer is provided internet banking facility, which would include:

- | | |
|----------------------------|-------------------------------------|
| a) Password change | e) Stop payment |
| b) Balance inquiry | f) Copy of statement of account |
| c) Fund transfer | g) ATM/ Credit Card related queries |
| d) Request for cheque book | |

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

Applicable Regulatory & Compliance Requirement

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:- <table><tr><td>i) Efficiency</td><td>v) Integrity</td></tr><tr><td>ii) Effectiveness</td><td>vi) Availability</td></tr><tr><td>iii) Reliability</td><td>vii) Compliance</td></tr><tr><td>iv) Confidentiality</td><td></td></tr></table> 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:- <table><tr><td>i) Configuration</td><td>iii) Transactions</td></tr><tr><td>ii) Masters</td><td>iv) Reports</td></tr></table>	i) Efficiency	v) Integrity	ii) Effectiveness	vi) Availability	iii) Reliability	vii) Compliance	iv) Confidentiality		i) Configuration	iii) Transactions	ii) Masters	iv) Reports	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)
i) Efficiency	v) Integrity														
ii) Effectiveness	vi) Availability														
iii) Reliability	vii) Compliance														
iv) Confidentiality															
i) Configuration	iii) Transactions														
ii) Masters	iv) Reports														

CORE BANKING SYSTEMS (Chart 5.59)

I) Risk around CASA Process	II) Risks around Credit Card Process	III) Risk around Mortgage Process	IV) Risk around Treasury Process	V) Risk in Loans & Advances Process	VI) Risks w.r.t Data Centre & Network Operations	
a) Credit Line setup is unauthorized & not in line with banks policy.	a) Credit Line setup is unauthorized & not in line with banks policy.	a) Incorrect customer & loan details are captured which will affect overall downstream process.	a) Unauthorized securities setup in systems such as Front office/Back office	a) Credit Line setup is unauthorized & not in line with banks policy.	a) Transaction may not be recorded completely or accurately, & related items will be inaccurately or incompletely recorded.	e) Timely execution & complete processing & availability of data may not be ensured
b) Customer Master defined in CBS is not in accordance with Pre- Disbursement Certificate.	b) Credit Line setup is unauthorized & not in line with banks policy.	b) Incorrect loan amount disbursed.	b) Inaccurate trade is processed.	b) Credit Line setup is unauthorized & not in line with banks policy.	b) Invalid items may be recorded or valid items may be inaccurately or incompletely recorded.	f) Unavailability of applications & data backups in event of a disaster. It can also result in disclosure of sensitive info
c) Inaccurate interest / charge being calculated in CBS.	c) Masters defined for customer are not in accordance with Pre-Disbursement Certificate.	c) Interest amount is incorrectly calculated & charged.	c) Unauthorized confirmations are processed.	c) Masters defined for customer are not in accordance with Pre-Disbursement Certificate.	c) Timely & adequate technical support may not be available & issues may not be resolved.	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.
d) Unauthorized personnel approving CA-SAS transaction in CBS.	d) Credit Line setup can be breached.	d) Unauthorized changes made to loan master data or customer data.	d) Insufficient Securities available for Settlement	d) Credit Line setup can be breached in Loan disbursement system/CBS.	d) User queries may not be timely & adequately resolved.	h) Backup may not be available
e) Inaccurate accounting entries generated in CBS.	e) Inaccurate interest / charge being calculated in Credit Card system.		e) Incomplete & inaccurate data flow between systems.	e) Lower rate of interest/ Comm may be charged to customer.		
	f) Inaccurate reconciliations performed.		f) Insufficient funds are available for settlements.	f) Facilities/Loan's granted may be unauthorized/inappropriate		
			g) Incorrect Nostro payments processed.	g) Inaccurate interest / charge being calculated in Loan disbursement system		

VII) Risks & Controls w.r.t Information Security		
a) Significant information resources may be modified inappropriately, disclosed without authorization, and/ or unavailable when needed.	d) Potential Loss of confidentiality, availability & integrity of data & system.	g) Potential loss of confidentiality, availability & integrity of data & system
b) Lack of management direction & commitment to protect information assets.	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.	h) Inadequate preventive measure for key server & IT system in case of environmental threat like heat, humidity, fire, flood etc.
c) User accountability is not established.	f) Unauthorized viewing, modification or copying of data and/ or unauthorized use, modification or denial of service in system.	d) Security breaches may go undetected.
d) Unauthorized system or data access, loss & modification due to virus		

VIII) Risks w.r.t Application Controls		
a) Interest may be incorrectly computed leading to incorrect recording of income/ expenditure.	f) Multiple liens in excess of deposit value may result in inability recover outstanding in event of a default.	i) Failure to automate closure of NRE/ NRO accounts on change in residence status may result in regulatory non-compliance & undue benefits to customers.
b) Inappropriate assignment of rate codes resulting in violation of business rules &/ or loss of revenue.	g) Inappropriate security or controls over system parameter settings resulting in unauthorized or incorrect changes to settings.	j) Failure to levy appropriate charges resulting in loss of revenue. Inappropriate levy of charges, resulting in customer disputes.
c) Absence of appropriate system validations may result in violation of business rules.	h) Inappropriate set up of accounts resulting in violation of business rules	k) Incorrect classification and provisioning of NPAs, resulting in financial misstatement.
d) Inappropriate reversal of charges resulting in loss of revenue.		
e) Failure to levy appropriate charges resulting in loss of revenue.		