New Additions and Changes in the ISCA Study for November 2015 Exam and Onwards

Dear Students,

The institute has introduced certain changes in the ISCA study for the November 2015 exams and onwards. The changes largely reflect further expansion of existing topics only. Conceptually and most of content of the study is similar to the last study. In addition, the institute has shifted the application and general controls topics from Chapter 6 to Chapter 3. The next few pages explain the new additions/changes in the study for the November 2015 exams and onwards.

Best for Exams

Chapter 1 Additions/Changes

In this chapter COBIT 5 is further expanded with the following new additions

Components in COBIT:

As we discussed earlier, COBIT is highly extensive framework and include best practices for the Information Technology management and related aspects. COBIT has evolved from a simple audit framework in 1996 to a comprehensive IT governance or GEIT (Governance of Enterprise IT) model.

COBIT 5.0 has the following key components:

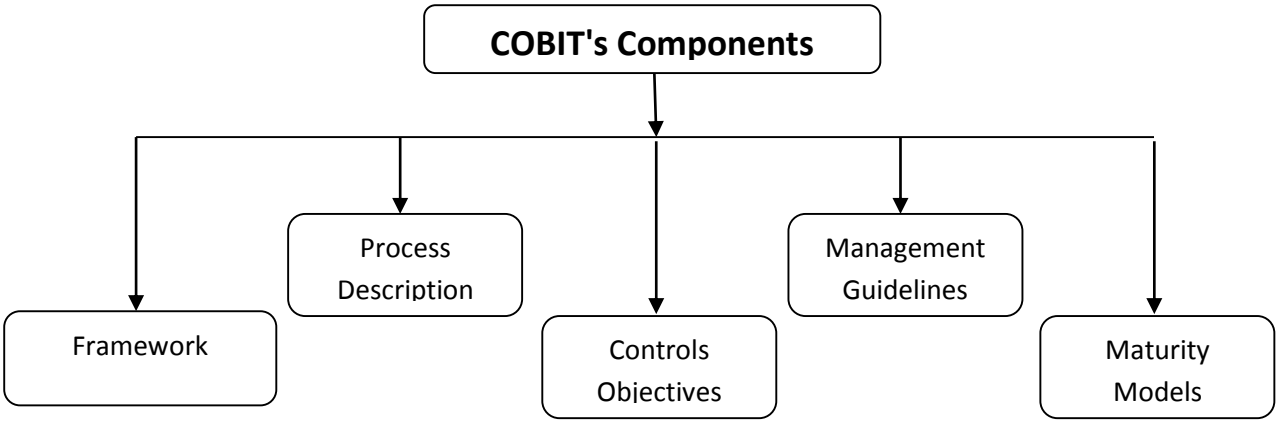
(i) Framework: It provides a comprehensive framework or best practices for IT Governance, IT Processes and links these to the business requirements.

(ii) Process Descriptions: It contains the reference process model for both governance and management of IT including planning, building, running and monitoring of information systems.

(iii) Controls Objectives: Provides effective controls guidelines and procedures to management for each IT process to meet controls objectives

(iv)Management Guidelines: Help to assign appropriate responsibility, agree on objectives, measure performance and provide relationships with other processes.

(v) Maturity Models: Helps to assess the maturity and capability of each process and address the gaps or helps to achieve maturity level ((or optimum level) for processes.



Benefits of COBIT:

This topic is similar to what we have already discussed in the "Need for COBIT" above. The following points describe the key benefits of COBIT:

- Provides comprehensive framework to enable organization to achieves objectives for governance and management of enterprise IT
- Provides best practices to help organization to create optimal value from IT by realizing maximum benefits and optimizing risks
- Helps to manage IT related risks and ensures compliance, continuity, security and privacy of information system.
- Helps in policy development and development of good practices for IT management
- Helps to increase user satisfaction for use of IT Services
- It is useful for all sizes of organizations and helps all sizes of organization for optimum use of IT resources
- COBIT supports for compliance to laws, regulations, contractual agreements and policies.

COBIT 5 Process Reference Model:

COBIT 5 includes a process reference model which describes number of processes for ***Governance*** and ***Management***. It provides a common reference model of processes understandable by both the information technology management and business management. However, COBIT describes that each enterprise should define its own process set by considering its own requirements. ***And, setting a common language for IT and business is key step to achieve good governance.*** This process reference model also provides framework for measuring and monitoring IT performance, providing IT assurance, communicating with service providers and integrating with best management practices.

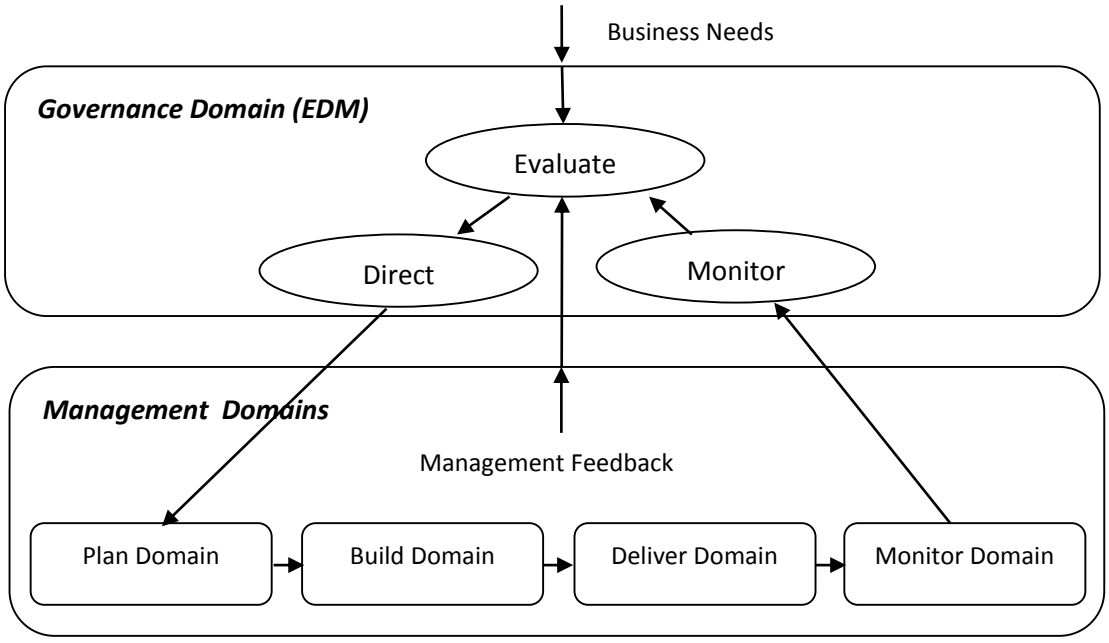
As discussed earlier, the COBIT 5 has a separate domain for governance and it has 4 domains for management of IT related activities. The figure below provides description of processes under Governance and Management domains. Here domain means areas under which large number of sub-processes or activities are defined related to that area.

Governance Processes:

It contains 5 processes EDM01 to EDM05. This domain is known as EDM or Evaluate, Direct and Monitor

Management Processes:

This contains large number of processes for IT development and management known as:
Align Plan and Organize (APO): It provides 13 processes from APO01 to APO13
Build Acquire and Implement (BAI): it contains 10 processes BAI01 to BAI10
Deliver, Service and Support (DSS): It contains the 6 processes (DSS01 to DSS06)
Monitor, Evaluate and Assess (MEA): It contains the 3 processes (MEA01 to MEA03)



COBIT 5 Governance and Management Domains

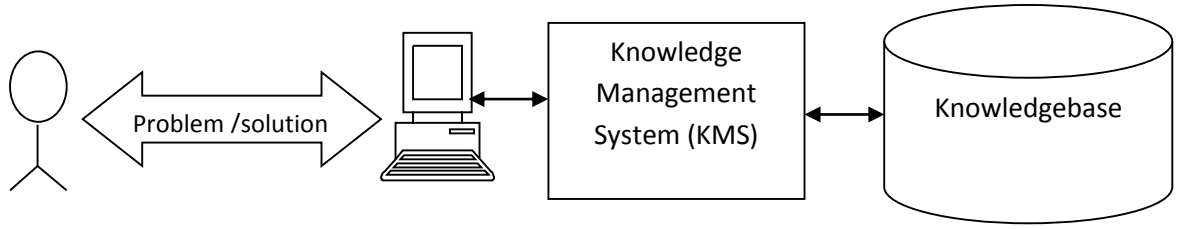
Chapter -2 Additions/Changes

The following new additions are there in this chapter and categories of information system is revised in the new study

Knowledge Management System:

We all know that world is becoming more and more a knowledge based economy and it is mostly dominated by organizations which can innovate new products and technologies e.g. Google, Apple, General Electric etc. A shift is happening where management is more concerned for intangible resources such as knowledge, technologies and competencies than tangible or physical resources such as equipment, machines and buildings.

Information and knowledge are the key elements of new economy. A firm's competitive gain in today's world depends on its knowledge processing i.e. what it knows; how it uses & how fast it can learn something new. Knowledge has become much more influential than land, labour and capital and it is true that world is moving in the direction of knowledge driven economies.



Let us learn a few key points about Knowledge Management Systems (KMS).

- KMS refers to an IT system which can store and retrieve knowledge.
- It improves collaboration and locates knowledge sources
- It mines repositories of data for hidden knowledge and captures and uses that knowledge
- KMS treats the knowledge component a precious resource and treat this as part of organization's explicit function just like finance and HR components are treated
- KMS provides an importance to knowledge component in organization such that it is reflected in strategy, policies and practices of the organization.

Knowledge can be divided into two broad categories—**Explicit** and **Tacit**

Explicit Knowledge:

- It is knowledge available in the documents and database of organization.
- It is collected through historical activities, operation and experience of organization.
- It is known as recorded knowledge
- It is represented in written material, compiled data and recorded audio and video data e.g. online tutorials, policies and procedure manuals etc

Tacit Knowledge:

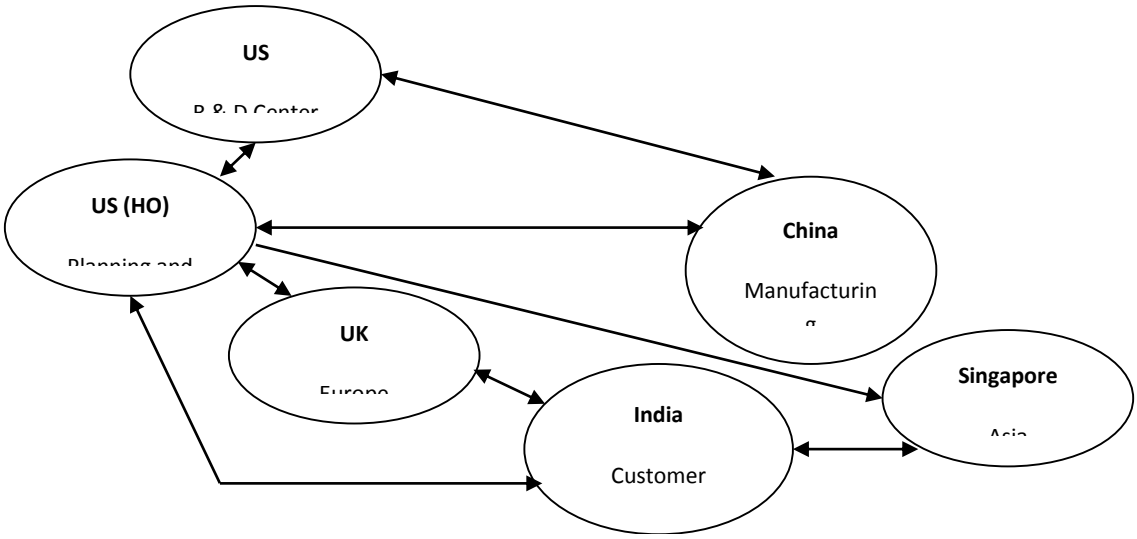
- It is known as personal knowhow. This is available through skills and experience possessed by organization's employees and advisors.
- This knowledge primarily resides in the mind of organization's employees
- This knowledge is represented as perspectives, understanding, intuition, belief and values that individual form based on their experiences.
- The tacit knowledge differentiates between organizations and provides strategic edge. It depends upon quality of professionals. For example, Micromax and Apple both manufacture the mobile phone devices but tacit knowledge of professionals in these two organizations differentiate these organizations

ERP (Enterprise Resource Planning)

- ERP provides solution to overall business problems.
- ERP helps to integrate five major resources of an organization namely: man, material, money, machine and market.
- ERP involves managing a large volume of data, large number of users and multiple system components distributed anywhere in the world.

A typical definition of ERP is like this: "software solutions that address the enterprise need by tightly integrating all functions of an enterprise". In simple words, ERP promises one database, one application and one user interface for entire enterprise, where previously separate systems ruled the manufacturing, personnel, finance and sales.

In general, ERP is a package software product but it is not a kind of software that can be installed immediately. ERP is a comprehensive system and provides solutions for business problems.
ERP is originated from Material Requirement Planning (MRP I) and Manufacturing Resource Planning (MRP II) which were comprehensive IT system and provided an integrated manufacturing and operational information systems. ERP further extended these systems by incorporating best business practices such as online, data mining and intranet and internet etc



A view of global business which can be managed using ERP

Components of ERP (components for ERP implementation)

This topic describes the components needed to implement ERP. ERM implementation primarily contains the following four components:

(i) Software Component: This is most important and most visible component of ERP. It contains various modules such as Finance, Supply Chain Management, Customer Relationship Management (CRM), Human Resources Management (HRM) and Business Intelligence.

(ii) Process Flow: This represents a model on how information flows between various modules to provide an integrated ERP system. This model also makes it easier to understand how ERP works.

(iii) Customer mindset: This is largely related to training to provide users awareness about the benefits of ERP to make them ready for use of new ERP system. Users generally resist while shifting to a new system because they are already well acquainted with an existing system therefore it is necessary that they should be trained and motivated for use of new ERP system.

(iv) Change Management: ERP implementation needs the changes to be managed at various levels, such as:

- Business Processes
- Procedures and methods for conducting activities
- User attitude and resistance for use of new system

Benefits of ERP:

ERP provides large number of benefits such as cost reduction for inventory and operations, integration of all business activities, efficient operation and better decision making. The key benefits of ERP can be as follow:

(i) It helps to integrate and streamline the processes and workflow
(ii) Provides a common integrated system across organization which helps to reduce the redundant date entry
(iii) Improve the workflow and efficiency
(iv) Improve customer services and satisfaction
(v) Helps to reduce the inventory costs by better planning, tracking and forecasting of requirements
(v) Decrease in vendor pricing by taking advantages of available pricing scheme and track the vendor performance
(vi) Track actual costs of activities or perform activity based costing
(vii) Provides a consolidated picture of sales, inventory and receivables
(viii) Turn collection faster or helps for better receivable management
(ix) Establishes uniform processes across the organization

CORE (*Centralized Online Real-time Environment)* Banking System:

Banks are the most active and biggest users of information technology and computer based information systems. We cannot imagine banking without use of computers and related applications. Information technology has allowed the online banking systems which help to provide banking from anywhere at any time.

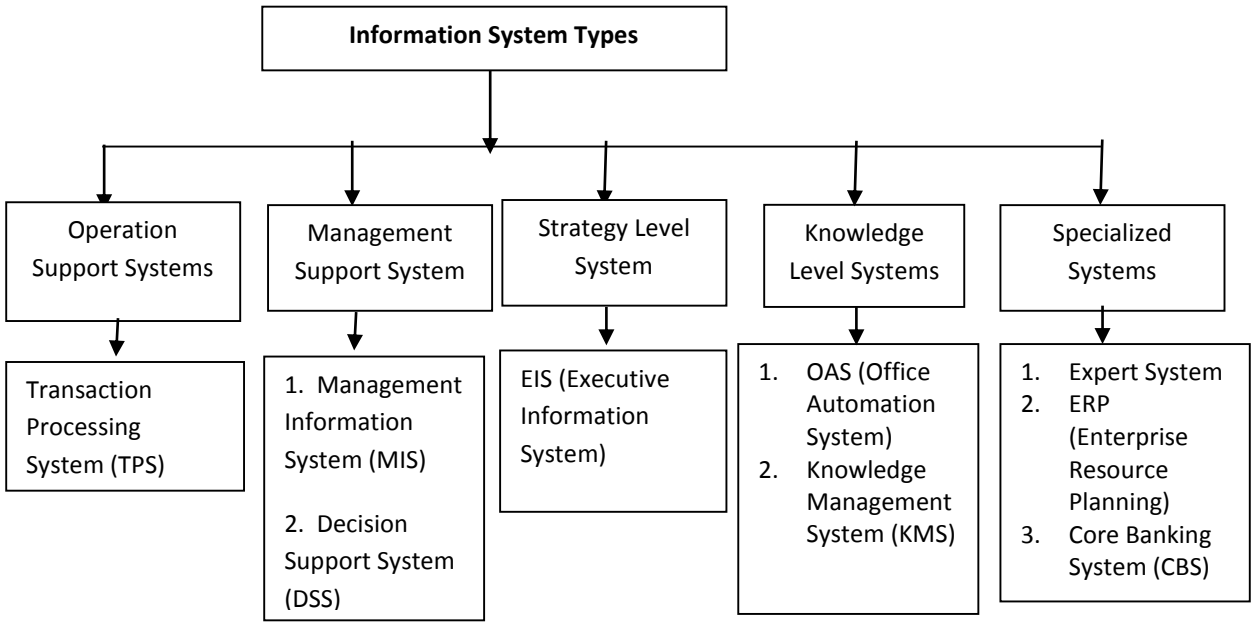
Nowadays most banks use CORE banking applications where CORE stands for ***Centralized Online Real-time Environment***. The CORE banking system has become a heart of banking system. All the bank branches, ATMs and Net Banking system access a centralized data centre. All the transactions of banks are recorded through this centralized data centre. The data centre remains available on 24x7 basis and can be accessed through net from anywhere which allow to conduct banking transactions at any time and from anywhere.

Information technology and communication technologies have merged to suit needs of banking is known as **CBS or Core Banking Solutions.** The technologies have reduced the downtime of banking systems and have increased the banking services performance. In CBS, the banking software or application is developed to perform core operations such as recording of transactions, passbook maintenance and interest calculations on loans and deposits, information about customer records for balance and withdrawal etc. Core banking functions are now linked to bill payment, tax payments and fund transfers and investment as well.

The key elements of CORE banking are:

- Opening new accounts
- Processing deposits and withdrawal
- Processing payment and cheques
- Loan Services
- Calculating interest and setting up interest rates
- CRM
- Managing customer and corporate accounts
- Establishing criteria for minimum balances, interest rates, number of withdrawals allowed etc
- Passbook management
- Maintaining records of all banking transactions

Also, types of information systems in the chapter are categorized as below:



Chapter 3 Additions/Changes:

These were my general observations for the previous study that Chapter 3 (Protection of Information System) and Chapter 6 (Audit of Information System) should be in continuity and controls related topics in chapter 6 of previous study should be in the Chapter 3. The Institute has removed that controls topics from Chapter 6 and has shifted those topics in the Chapter 3. The Chapter 6 is now fully focused on Audit of Information System. Also, the new additions in the chapter 3 are not very different than the existing controls topics.

The following new additions are there in the Chapter 3 and all the controls related topics from the previous study are shifted from Chapter 6 to this chapter.

Impact of Technology on Internal Controls:

This is a kind of repetitive topic and very much similar to the "Information Technology Impact on Internal Controls". The following are the key impacts of technology on internal controls. These impacts primarily explain the difference between manual system and computerized system

(i) Competent and Trustworthy Personnel: The persons working in technology environment should have appropriate knowledge of IT systems working to discharge their duties.

(ii) Segregation of Duties: In manual system auditor is normally concerned with the segregation of duties of finance department as data is prepared and processed at that place only, whereas in computerized system auditor remains concerned for segregation of duties in both finance and IT departments as both the departments have access for data.

(iii) Authorization Procedures: In computerized environment, supervisor authorization of manual system is replaced with automated procedures implemented within the computer programs.

(iv) Adequate Documents and Records: In manual system, adequate documents and records are needed to provide audit trail of activities. In computerized system no visible trail exists to trace the transactions.

(v) Physical Controls over Assets and Records: It is important to implement physical controls for protection of assets in both manual and computerized systems. In manual system protection of assets and records are implemented using locked doors and filing cabinets. In the computerized systems new types of controls are needed as data is normally maintained at one centralized location and this increases the losses that can arise from computer abuse or a disaster.

(vi) Adequate management Supervision: In the manual system management supervision is straightforward as both managers and employees are often at the same physical location. However, in the computerized systems the employees may be based at remote locations thus supervision might be carried out remotely.

(viii) Independent Checks of Performance: In computerized system the independent checks of performance are easy to implement and track as these are implemented using program codes and there are

less chances of errors. In the manual system, employees may be careless or intentionally can do the errors or may forget the procedures and can do the errors. Thus independent checks of performance need to be regularly carried out for the manual system.

(viii) Comparing Recorded Accountability with Assets: It is important to check the accuracy of recorded data with the assets the data represent by comparing the data with actual available assets. In the manual system this comparison is performed by staff while in computerized system the comparison data is prepared using software but comparison with actual assets is performed by staff.

(ix) Delegation of Authority and Responsibility: Delegation of authority and responsibility is an important control. In the manual system it is to implement this control while in computerized system it may be slightly difficult as same resources are shared among multiple users.

Classification of Information System Controls:

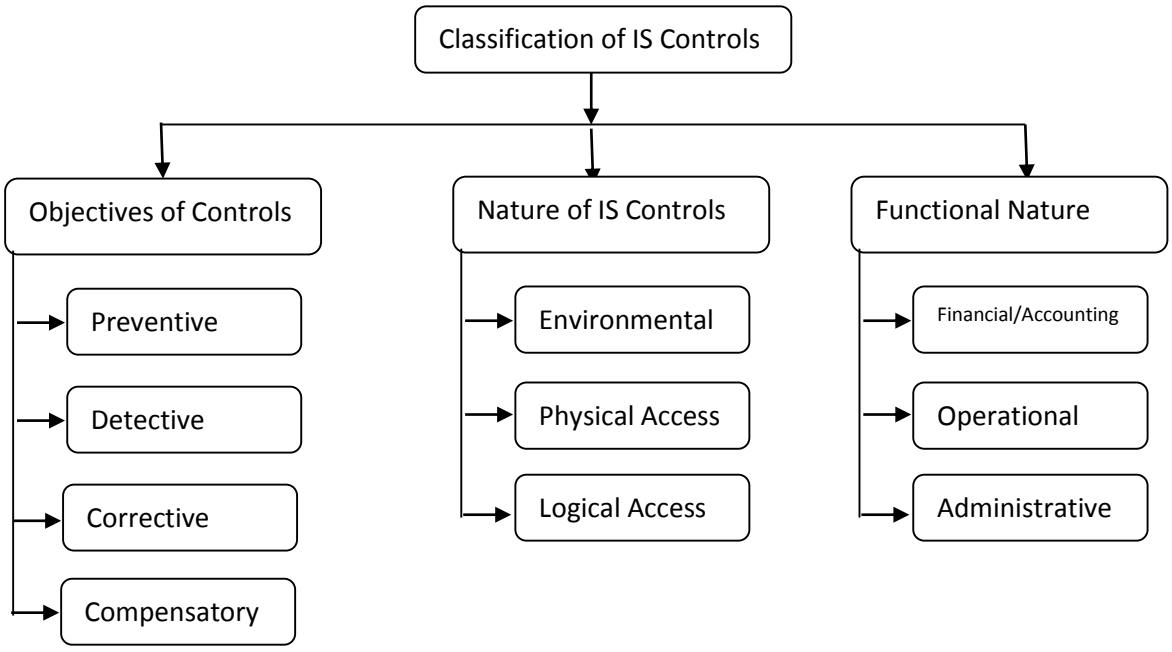
In the previous study, the information system controls were classified in the three categories as:

(i) Objectives of Controls
(ii) Nature of IS Controls
(iii) Functional Nature of Controls

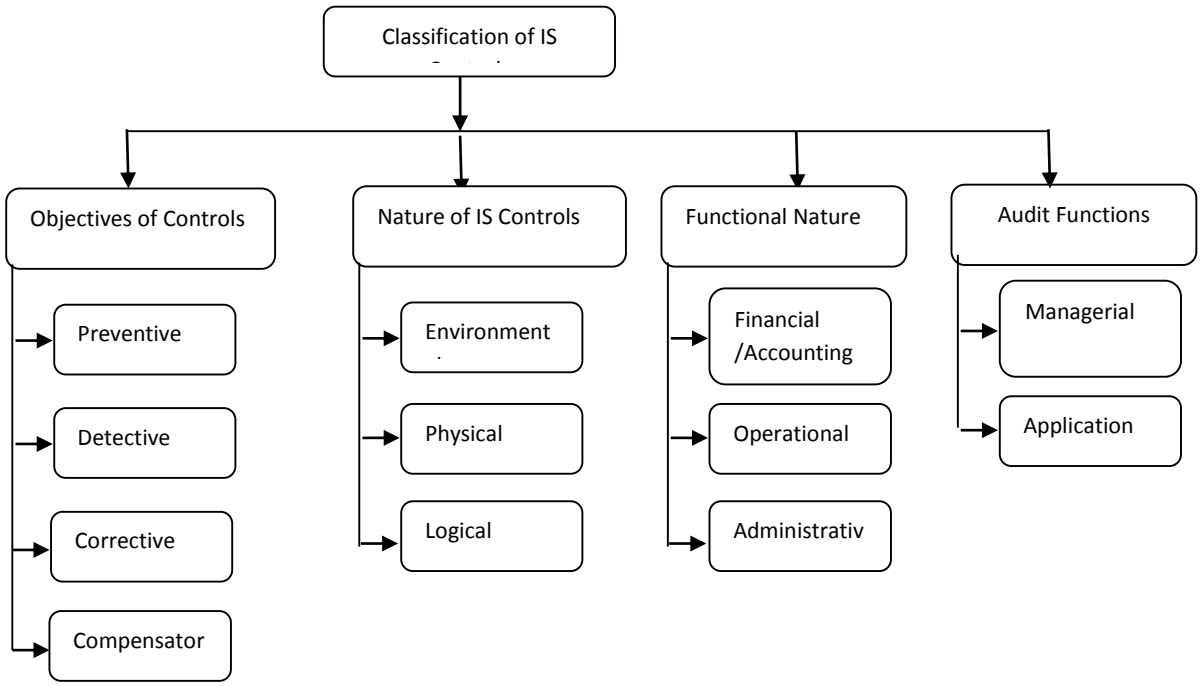
In the new study, the classification of information system includes the four categories as:

(i) Objectives of Controls
(ii) Nature of IS Controls
(iii) Functional Nature of Controls
(iv) Controls as per Audit Functions

Controls Classification in the Previous Study:



Controls Classification in the Latest Study:



Classification on the Basis of Audit Functions: This classifications is based on how auditor conduct the audit of controls and this includes the following types of controls

(i) Managerial Controls: This includes controls over managerial activities to ensure that information system is planned, developed, implemented and used in a controlled manner. The controls at this level help to provide a reliable and efficient information system for day-to-day activities.

(ii) Application Controls: This includes the controls within the program codes of application. The objectives of these controls are to ensure data is complete, accurate and valid. It also ensures that data backup and recovery procedures are in place to recover data in case of any disaster. These controls also ensure confidentiality, privacy and integrity of data.

17.1 Managerial Controls Types: (New topic for Nov 2015 Exam)

(i) **Top Management Controls:** The top management should be involved in setting-up the policy and rules to ensure that information system is well managed

(ii) **Information system management (IS Management) Controls:** This IS management is direct responsible for managing and setting up controls for information system. The IS management advices the top management for setting up policy and rules for efficient management of information system.

The top management and IS Management are primarily involved in the following functions:

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

Planning is the most important function of top management. The top management and IS management should develop two types of information system plan: strategic plan and operation plan. The strategic plan is long-term plan for information system management and operation plan is a short-term plan for information system management.

(iii) **System Development Management System:** This management is responsible for the design, implementation and maintenance of application and information system:

Auditors can play very important roles in the system development. They can conduct different types of audit for system development.

General Audit: To check whether the developed system is efficient, accurate and reliable and provide audit opinion about system efficiency, effectiveness and correctness of financial statement it produces to management

Concurrent Audit: In this, auditors become the members of audit team and they assist the development team improving quality of system development for the system team is building

Post-Implementation Audit: over here auditors check whether the system developed is providing the desired results and expected performance. This audit helps organization to learn from its system development experiences and also help to determine whether to continue with the new system or scrapped the system.

(iv) **Programming Management System Controls:** This management is responsible for programming or developing application of new system or updating the application of existing system.

Programming development is a task within the system development life cycle phases. The key purpose of programming development is to produce acquire and produce the high quality programs. The programming development life cycle comprises the following six phases.

Planning Phase: This includes planning of time, costs and resources for the program development activities. The Work Breakdown Structure (WBS), Gantt Charts and PERT chart can be used for planning and monitoring progress of activities.

Design: It includes a systematic approach to design programs by using flowcharts and object oriented tools.

Coding: Programmers can develop programs in modules and can use an integration strategy for modules such as top-down or bottom-up approach and can also ensure that documentation is prepared for each task.

Testing: The programmer can use (i) Unit Testing (ii) Integration Testing and (iii) whole Program testing to ensure program is accurate and working as specified.

Operation & Maintenance: As described in the Chapter 5 in the system maintenance phase, there can be different maintenance approaches for program maintenance also such as: **Repair maintenance:** In this program errors are corrected. **Adaptive Maintenance:** In this programs are modified to meet the changing requirements. **Perfective maintenance:** In this program is improved for better performance.

Controls: This includes using controls in all the above phases and it ensures the controlled development and maintenance of programs.

(v) **Data Resource Management and Administration Controls:** Data administrator is responsible for planning and controls issues related to data for example who can access what data and why etc. Data resource management controls includes backup and recovery procedures to ensure that data is available in the adverse situation also.

(vi) **Quality Assurance Management Controls:** This management ensures that information system development complies to the established or desired quality standards such as ISO 9001 and uses best practices such of COBIT

(vii) **Security Management Controls:** It is responsible for planning access controls and physical security of information system assets. The controls are needed for the threats such as fire, water damage, energy variation, pollution, unauthorized intrusion, viruses, misuse of software and hacking etc

(viii) **Operations Management Controls:** This management is responsible for planning and control of day-to-day operation of information system. This management typically apply the controls such as help desk for technical and services support, capacity planning and performance monitoring etc.

Application Controls and their types:

These controls are shifted from the Chapter-6 to Chapter 3 and added two new controls in this as Processor controls and communication controls

Application controls can be classified as:

- Boundary Controls:
- Input Controls
- Data Processing Controls
- Output Controls
- Database Controls
- Processor Controls
- Communication Controls

Processor Controls:

The processing system is responsible for computing, sorting, classifying and summarizing data. The major system components of processing system are central processor (CPU), RAM, virtual memory and operating system. The controls should be there for these components to ensure error free data processing.

Central Processor Controls:

The central processor known as CPU (Central Processing Unit) is the most important component of computer and it contains the three main components:

Control Unit: It fetches the data and instructions from memory and provide that to processor for processing

Arithmetic Logical Unit: This performs the arithmetic and logical operations on data provided by Control unit.

Registers: Registers are memory units of processor and store the results temporarily during processing.

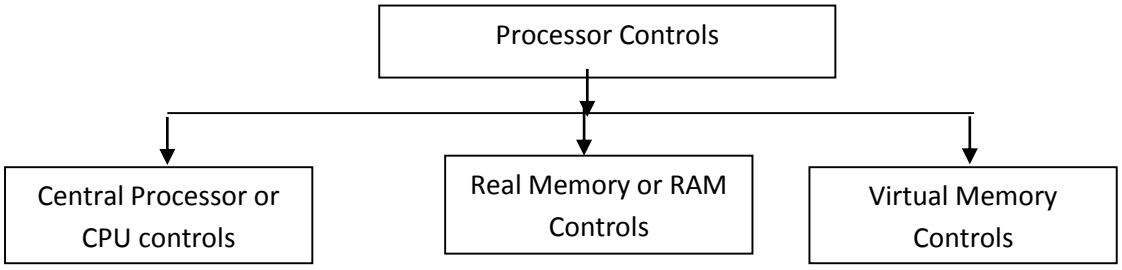
The central processor is controlled by operating system and apply different controls to reduce the errors related to central processor operation. The OS implement the features or controls such as Error Detection and Correction Control, Multiple Execution Control and Timing Control for central processor.

Real Memory Controls or RAM controls:

This memory is used to store those data and instructions which are under execution or being used by central processor. The controls related to real memory include detection and correction of errors which may occur while loading program in RAM and also protect memory from illegal/unauthorized programs such as virus access. These controls are also provided by operating system for RAM.

Virtual Memory Controls:

The virtual memory exist when required space for programs/data execution is larger than available RAM space. The operating system implement virtual memory controls to ensure the correct mapping of virtual memory with RAM to ensure correct execution of large size or multiple programs using virtual memory.



Communication Controls:

These controls are related to error free, reliable and secured communication of data

The major risks in communication system are:

(i) Transmission Errors (due to technical issues)
(ii) Components Failure (Failure of Modem, Channels)
(iii) Subversive activities – Hacking etc

We have discussed controls due to components failure and subversive activities in the general controls section below. Here we will study technical aspects of transmission system and possible controls.

(i) **Physical component Controls:** These controls incorporate the features that mitigate the possible exposure for the following communication devices:

Transmission Media or Communication Channel: There can be two types of transmission media: (a) Guided or wire channels such as co-axial, twisted pair cable and optical fiber (b) Un-guided or wireless channels such as radio frequency, microwave and satellite.

Appropriate selection of communication channel helps to improve the reliability and data speed of data communication

Modem: Modem is used to modulate/de-modulate or transmit the computer data on communication channel. Modem used should be able to detect and correct errors due to connection with communication channel.

Multiplexor: This is used to share the bandwidth of a channel by many devices for data communication. Multiplexor should be able to avoid any congestion, slow speed and reliability issues due to this sharing of channel bandwidth.

(ii) **Line Error Control:** This includes controls which help to detect and correct errors in communication lines due to noise or disturbances. The controls such as Echo check and CRC (Cyclic Redundancy Check) are used to detect and correct line errors.

(iii) **Flow Controls:** If data sending rate and receiving rate for communication is different then data flow errors can be there. For example, a high speed device sending data to low speed device can cause data flow errors. In this case, a flow control mechanism can be introduced to ensure error free flow of data or controlling speed of devices to match sending rate with receiving rate.

(iv) **Link Controls:** A link primarily reflects the linking of two devices or nodes using communication channel and devices. Any inappropriate linking may result in data communication errors and speed issues and thus the devices should be properly linked and synchronized to avoid any linking errors.

(v) **Topological Controls:** Specifying appropriate topology or structure is highly important for a network. The optimum topology selection helps to improve reliability and data communication speed. The topology are generally selected as per area coverage network such as:

a. **LAN (Local Area Network) Topologies:** LAN is a privately owned, high speed and confided to a limited area or a building network. LANs are generally implemented using the following topologies: (i) Bus Topology (ii) Tree Topology (iii) Ring Topology (iv) Star Topology and Hybrid like Star-ring and Star-bus etc.

b. **WAN (Wide Area Network) Topologies:** WAN is a network owned by other parties such as telecom organizations, provide slower speed communication than LAN and span over a large area. WAN can use all other topologies as LAN except the Bus topology.

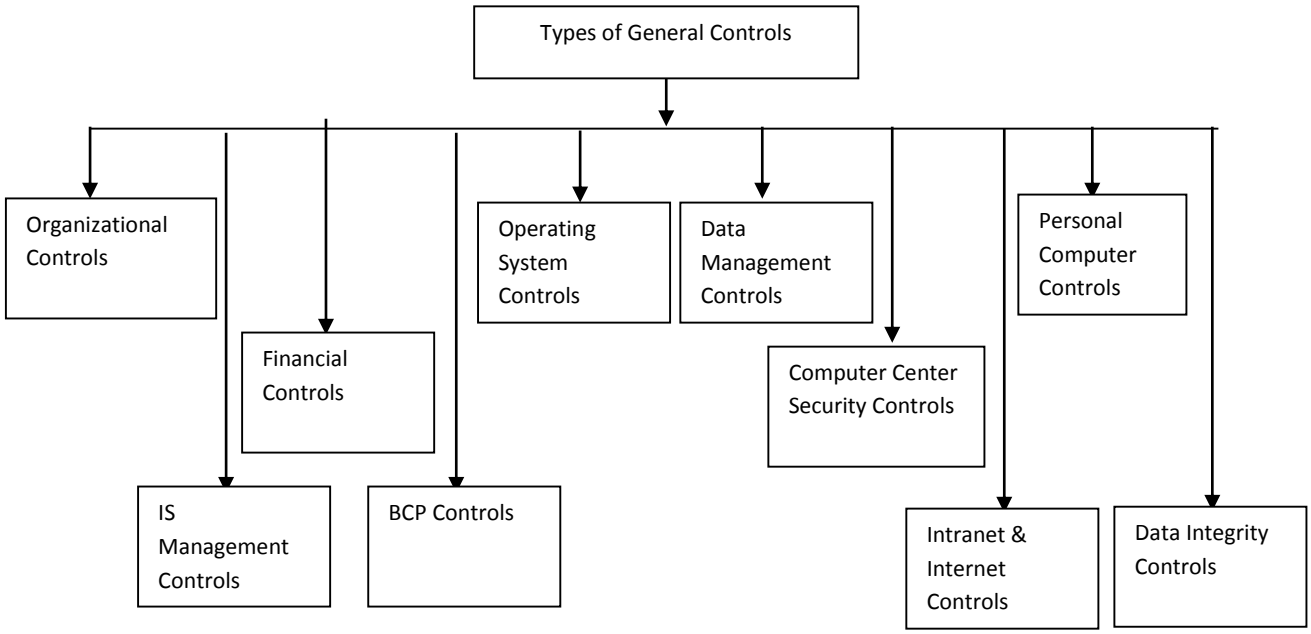
(vi) **Channel Access Control:** It is very common that multiple devices compete to gain access for a common communication channel for data communication. Two methods are used for

channel access: **(a) Polling Method:** This is a technique in which an order or sequence is established for the connected devices for the channel capacity access. **(b) Contention Method:** In this each connected device request for access and based on pending requests from other devices the channel access is granted. Appropriate controls should be there to avoid failure in granting access or reliability issue in channel access.

(vii) **Internetworking Controls:** Internetworking is a process of connecting two or more networks together. Internetworking is a complex issue and controls should be there to avoid possible errors or reliability issues due to internetworking. The most common devices used for internetworking are: **(a) Bridge:** A bridge is used to connect two similar networks i.e. ring network with ring network **(b) Router:** It is an extension of bridge and can connects multiple different networks with each other **(iii) Gateway:** Gateway is further extension of router and allows any architecture or network type to be connected with each other and it allows protocol conversion from one type of network to other.

Types of General Controls:

These controls are largely shifted from the Chapter 6 to this chapter. The general controls are those controls which help to maintain IT infrastructure in a reliable and efficient form. The following general controls types are there in the study

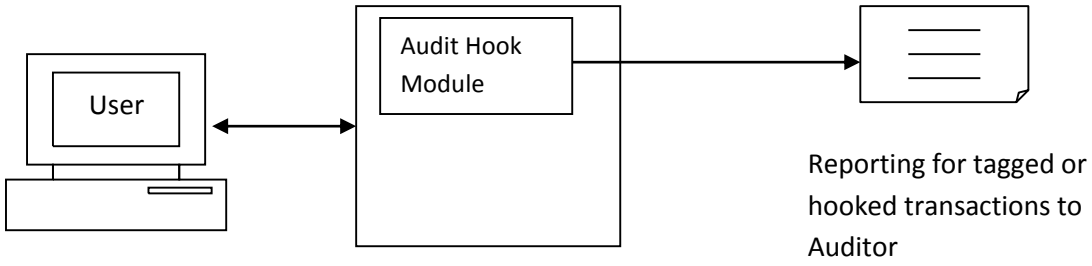


Chapter 6 Additions/Changes:

In the concurrent or continuous audit system a new technique known as Audit Hook is added

Audit Hook

This audit technique helps to flag suspicious transactions. In this technique, the known methods of frauds are tagged or hooked for detecting frauds. For example, if transactions conducted for printing and stationary accounts involves maximum frauds then auditor will tag the transactions conducted with title printing & stationary and these are flagged for possible frauds. This is similar to SCARF technique but act for more specific transactions to detect the possible frauds.



Application Controls and Audit Trails (New Topic for Nov 2015 Exam)

We have already discussed the application controls in Chapter 3 such as Boundary Controls, Input Controls, Data Processing Controls, Output Controls, Database Controls, Processor Controls and Communication Controls

There are two types of audit trails which exists in a system:

(i) Accounting Audit Trail: This maintains a record of events for system under observation
(ii) Operation Audit Trail: This maintains record of resource consumption associated with each event

Application Control	Description	Accounting Audit Trail	Operation Audit Trail
Boundary Controls	Maintain sequence of events related to user entry into system and provide access as per user rights and authorization	Maintains record on access allowed or disallowed to users	Maintain log on resources used during each access
Input Controls	Maintain sequence of events related to inputs captured and entered into an application system until these are validated for processing	Maintain log on transactions or inputs: who entered, what entered, date and time of entry, type of device used for input etc.	Maintain log on application used, total time application and devices used for input and any errors etc.
Data Processing and Processor Controls	Maintain the sequence of events from the time data is received for processing to results are dispatched to the database, communication devices or output	Maintain sequence of processing steps. Monitor input data entry, intermediate results and output data values.	Maintain log on hardware use such as CPU time, RAM etc. and maintain log on software use such as compilers and subroutine libraries used and files used etc.
Output Controls	Maintain sequence of events from the time output is generated and delivered	Maintain log on what output is generated and who received that and when, and what actions were taken on output	Maintain log on resources consumed for outputs– graphs, images, pages, printing time and display used.
Database Controls	Maintain the sequence of events that occur for data storage, backup and updation	Maintain a unique time stamp such as time, date for transactions recorded in database and maintain details who recorded/saved the data	Maintain log on resource consumption such as storage space and database files
Communication Control	Maintains a sequence of the events from the time a sender sends a message to the time a receiver receives the message.	Maintain log on each node involves: which node send and revive messages with user id and time and date at which the messages were sent and received, and message id etc.	Maintain log on network devices used for communication with time, and errors occurring on each node or retransmissions with device restarts happen.

Chapter -7 Additions/Changes

In this chapter ISO 27001 and ITIL V3 topics are revised with the following additions

How Information Security Standard ISO 27001 works?

ISO 27001 standard requires that management

- systematically examines the organization's information security risks taking into the account the threats, vulnerabilities and impacts
- design and implement a coherent suite of information security controls and risk treatment and addresses those risks which are unacceptable
- adopt management processes to ensure that information security controls continue to meet the organization's information security needs on an ongoing basis.

History of ISO 27001:

- ISO/IEC 27001 is emerged from the British BS 7799 Part 2, published in 1999.
- BS 7799 part 2 was further revised by BSI in 2002 by incorporating Deming's PDCA process concept and was finally adopted by ISO/IEC as ISO/IEC 27001 in 2005.
- It was further revised in 2013 by bringing in other ISO management standards. The ISO/IEC 27001 is part of growing ISO/IEC 27000 family of standards.

ISO: International Organization for Standardization
IEC: International Electrotechnical Commission
PDCA: Plan-Do-Check-Act

ISO/IEC 27001:2013:

It is the first extensive revision of ISO/IEC 27001 that specifies for establishing, implementing, maintaining and continually improving the information security management system for organization. It also includes requirements for the assessment and treatment of information security risks as per the needs of organization. The ISO/IEC 27001:2013 is applicable for all type and size of organizations. The ISO/ICE 27001:2013 was published in September 2013.

Structure of ISO 27001: 2013:

In the new structure the PDCA model used in ISO 27001:2005 was dropped. The reason was PDCA could provide the just one approach for meeting continual improvement requirements. In the ISO 27001:2013 new approaches are introduced which organization can use as per the requirements.

The structure of ISO 27001:2013 has a ten clauses plus a long annex as discussed below:

Clause 1: Scope
Clause 2: Normative References
Clause 3: Terms and Definitions
Clause 4: Context of the organization
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement

Annex A: List of controls and their objectives
ISO/IEC 27001:2013 specifies total 114 controls in 14 in groups A.5 to A.18 in contrast to 133 controls in 11 groups in the old standard
A brief descriptions of A.5 to A.18 are shown below:

Annex	Control Name	No. of Controls
A.5	Information Security Policy	2
A.6	Organization of information security	7
A.7	Human Resource Security (for before, during and after employment)	6
A.8	Asset Management	10
A.9	Access Controls	14
A.10	Cryptography	2
A.11	Physical and environment security	15
A.12	Operation Security	14
A.13	Communication Security	7
A.14	Information System Acquisition, development and maintenance	13
A.15	Relationship with external parties	5
A.16	Information security incident management	7
A.17	Information security in business continuity management	4
A.18	Compliance with legal and contractual requirements	8

Changes in ISO 27001:2013 from ISO 27001:2005:

The new ISO 27001: 2013 put more thrust on measuring and evaluating how well an organization's ISMS is performing. It also focuses on outsourcing risks. The outsourcing of services has become highly important aspect in the market and security risks related to outsourcing is another important consideration which need to be tackled. The ISO27001:2013 has

a new section on outsourcing. Overall, ISO:27001: 2013 is designed to fit better alongside other management standards such as ISO 9000 and ISO 20000.

ITILV3 (IT Infrastructure Library) (Revised for Nov 2015 Exam and onwards)

The following additional points are added to the ITILV3 books

(1) Service Strategy Components:

Service Strategy contains the following key components:

(i) IT Service Generation: It is related with implementation and management of quality IT services. It is performed through people, process and information technology
(ii) Service Portfolio Management: IT portfolio management is application of systematic management of investments, projects and activities of IT departments
(iii) Financial Management: The aim of this component is to provide accurate and costs effective management of IT assets and resources
(iv) Demand Management: This is used to manage and forecast the demand of products and services
(v) Business Relationship Management: This is formal approach for understanding, defining and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services vis network

(2) Service Design Components

Service Design contains the following key components:
(i) Service Catalogue Management: This maintains detail of all services available to customers. It includes ordering and requesting process from customers and delivery process and prices from company.
(ii) Service Level Management: It helps to identify, monitor and review the level of services as per Service Level Agreement. This ensures that agreed services are delivered
(iii) Availability Management: This ensures that IT services are available on 24x7 basis or available at agreed level at a justifiable cost. This addresses IT services features such as reliability, maintainability, serviceability and security provided at agreed level of services over a period of time
(iv) Capacity Management: This supports the cost effective and optimum IT services. This includes creating appropriate application size, workload/demand management and resources management to provide efficient services to users
(v) IT Service Continuity Management: This ensures that processes are in place which help to recover the IT immediately in case of failure or serious incident.
(vi) Information Security Management: This ensures that adequate security is in place to protect assets against possible risks. This primarily ensures confidentiality, integrity and availability of data when required including achieving goals such as authenticity and accountability and reliability.
(vii) Supplier Management: The purpose of this process is to obtain value from suppliers/services contracts which organization has entered. This ensures that the company entering into contracts with suppliers has synchronized the contracts with its service level agreements the company is offering to its customers.

(3) Service Transition Components

Service Transition contains the following key components:

(I) Supplier Transition Planning and Support: This ensures an orderly transition to new service into operation. It also ensures that necessary supports for services will be in place.

(ii) Change Management and Evaluation: This aims that standard methods and procedures are used for handling all changes. A change represents event which results in new configuration items which can be more cost effective and efficient in operation. For example change from a simple software to ERP software.

(iii) Service Asset and Configuration Management: This includes maintaining list of assets and associated configuration to deliver the services efficiently.

(iv) Release and Deployment Management: This requires managing the distribution of software and hardware including license control. This ensures controls exist for managing software licenses and hardware in the IT infrastructure

(v) Service Validation and Testing: This ensures that deployed software and associated services will work as per requirements and will meet the customer expectations

(vi) Knowledge Management: This involves capturing, developing and effectively sharing organizational knowledge.

(4) Service Operation Components

Service Operation contains the following Major Functions:

(i) Service Desk: This is very important element of IT services. This provides a single point of contact (SPOC) for all the customers. The service desk includes handling requests and providing interface for all the IT related processes.

(ii) Application Management: This includes managing the application software with best practices to improve the overall quality of software.

(iii) IT Operations: It includes putting the processes in place for output management, job scheduling, backup, restore, database management and network management.

(iv) Technical Support: This provides number of specialist functions such as market intelligence, data mining, research and evaluation etc.

(v) Incident Management: This aims to restore normal services and operation as soon as possible to avoid the adverse effect on business operation.

(vi) Request Fulfilment: This includes fulfilment of user requests such as change in password or request for information.

(vii) Event Management: An event may indicate that something is not functioning correctly. Event management generates and detects notifications while monitoring status of different components of IT system.

Chapter 4, 5, and 8 of study are not changed