Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

Chap 1

Page 1.27

1.10.3 Components in COBIT

• Framework - Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements.

• Process Descriptions - A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.

• Control Objectives - Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

• Management Guidelines - Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.

• Maturity Models - Assess maturity and capability per process and helps to address gaps.

Page 1.28

1.10.4 Benefits of COBIT 5

COBIT 5 frameworks can be implemented in all sizes of enterprises.

• A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.

• The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

• Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.

• COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.

• COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.

• The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

• COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

Chap 2

Page 2.15

2.2.5 Types of Information System

(B) Knowledge Management System (KMS) –

The world is moving swiftly in the direction of a knowledge-based system as enterprises adapt more and more cost- cutting measure. There is a paradigm shift from an economy principally concerned by the management of tangible resources (equipment, machinery, buildings, ...) to an economy in which renovation and growth are determined by intangible resources and investments (knowledge, technology, competencies, abilities to innovate....). Information and Knowledge are the key elements of this economy. A firm's competitive gain depends on its knowledge processing i.e. what it knows; how it uses & how fast it can know something new. It's much more influential than the harmony of land, labour & capital (i.e. three most important production factors). Even though there is not a lucid and exclusive definition of the so-called knowledge-based or knowledge-driven economy, it seems to be unstated as the 'upshot of a set of structural changes'.

Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organizational knowledge. It refers to a multi-disciplined approach to achieving organizational objectives by making the best use of knowledge. Knowledge Management Systems (KMS) refers to any kind of IT system that stores and retrieves knowledge, improves collaboration, locates knowledge sources, mines repositories for hidden knowledge, captures and uses knowledge, or in some other way enhances the KM process. KMS treats the knowledge component of any organization's activities as an explicit concern reflected in strategy, policy, and practice at all levels of the organization.

There are two broad types of knowledge - Explicit and Tacit as shown in the Fig. 2.2.5. KMS makes a direct connection between an organization's intellectual assets — both Explicit [recorded] and Tacit [personal know-how] — and positive results.

♦ **Explicit knowledge:**

Explicit knowledge is that which can be formalized easily and as a consequence is easily available across the organization. Explicit knowledge is articulated, and represented as spoken words, written material and compiled data. This type of knowledge is codified, easy to document, transfer and reproduce.

For example – Online tutorials, Policy and procedural manuals.

♦ **Tacit knowledge:**

Tacit knowledge, on the other hand, resides in a few often-in just one person and hasn't been captured by the organization or made available to others. Tacit knowledge is unarticulated and represented as intuition, perspective, beliefs, and values that individuals form based on their

experiences. It is personal, experimental and context-specific. It is difficult to document and communicate the tacit knowledge.

For example – hand-on skills, special know-how, employee experiences.

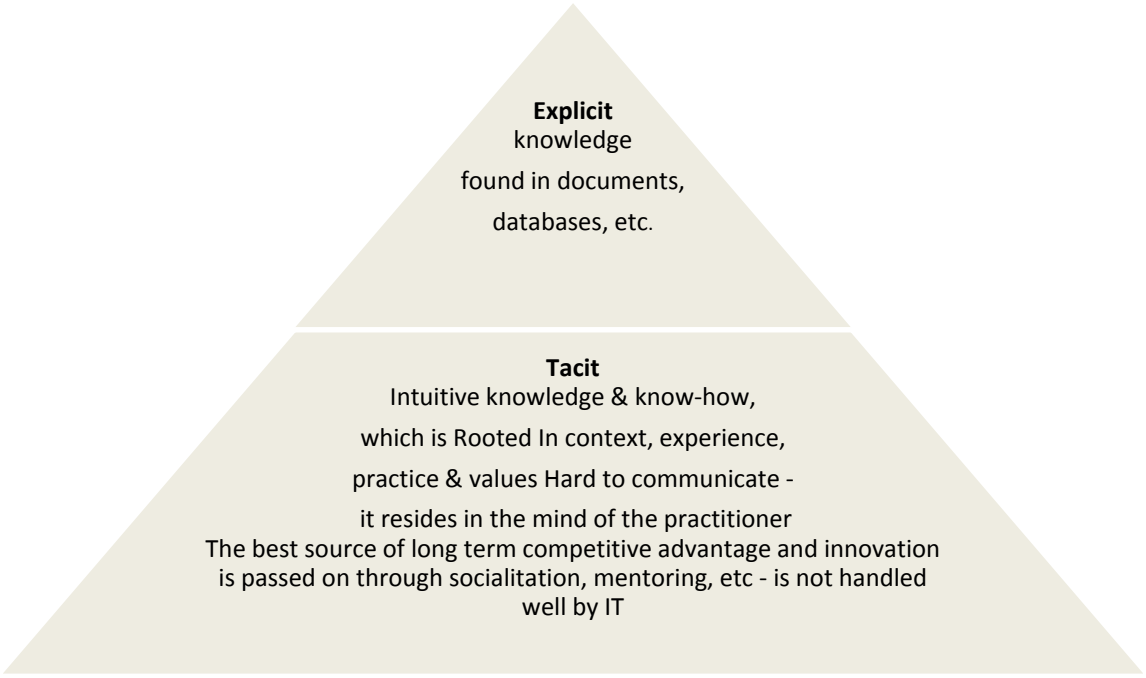


Fig. 2.2.5: Types of Knowledge

It is this tacit knowledge that differentiates between organizations when push comes to shove, and hence provides the strategic edge to any organization. A regular example in the software industry is how to write code to get around a particular limitation, or to include a particularly tricky condition.

Page 2.31

2.2.6 Specialized System

(B) Cross Functional Information Systems –

It is also known as integrated information system that combines most of information systems and designed to produce information and support decision making for different levels of management and business functions.

Example – Enterprise Resource Planning (ERP).

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

Enterprise Resource Planning (ERP) –

Enterprise resource planning (ERP) is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back office functions related to technology, services and human resources. ERP software integrates all facets of an operation, including product planning, development, manufacturing, sales and marketing. ERP software is considered an enterprise application as it is designed to be used by larger businesses and often requires dedicated teams to customize and analyze the data and to handle upgrades and deployment. In contrast, Small business ERP applications are lightweight business management software solutions, customized for the business industry we work in.

(A) Components of ERP

ERP model is consists of four components which are implemented through a methodology. All four components are as follows:

(i) Software Component: The software component is the component that is most visible part and consists of several modules such as Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligent.

(ii) Process Flow: It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model makes it easier to understand how ERP work.

(iii) Customer mindset: By implementing ERP system, the old ways for working which user understand and comfortable with have to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellence job without help from ERP system. In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.

(iv) Change Management: In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.

(B) Benefits of ERP

- Streamlining processes and workflows with a single integrated system.
- Reduce redundant data entry and processes and in other hand it shares information across the department.
- Establish uniform processes that are based on recognized best business practices.
- Improved workflow and efficiency.
- Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
- Reduced inventory costs resulting from better planning, tracking and forecasting of

requirements.

o Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.

o Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.

o Track actual costs of activities and perform activity based costing.

o Provide a consolidated picture of sales, inventory and receivables.

(C) Core Banking System (CBS) –

Core Banking is a banking services provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices. Normal core banking functions will include transaction accounts, loans, mortgages and payments. Banks make these services available across multiple channels like ATMs, Internet banking, and branches.

Most commonly, Core Banking System (CBS) may be defined as a back-end system that processes daily banking transactions, and posts updates to accounts and other financial records. These systems typically include deposit, loan and credit- processing capabilities, with interfaces to general ledger systems and reporting tools. Core banking functions differ depending on the specific type of bank.

Examples of core banking products include Infosys' Finacle, Nucleus FinnOne and Oracle's Flexcube application (from their acquisition of Indian IT vendor i-flex).

Elements of core banking include:

• Making and servicing loans.

• Opening new accounts.

• Processing cash deposits and withdrawals.

• Processing payments and cheques.

• Calculating interest.

• Customer Relationship Management (CRM) activities.

• Managing customer accounts.

• Establishing criteria for minimum balances, interest rates, number of withdrawals allowed and so on.

• Establishing interest rates.

• Maintaining records for all the bank's transactions.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

Chap 3

Page 3.11

3.5.4 Impact of Technology on Internal Controls

These are discussed as follows:

• Competent and Trustworthy Personnel:

Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the errors responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations. Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task.

• Segregation of Duties:

In a manual system, during the processing of a transaction, there are split between different people, such that one person does not process a transaction right from start to finish. Various stages in the transaction cycle are spread between two or more individuals. However, in a computerized system, the auditor should also be concerned with the segregation of duties within the IT department. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output.

• Authorization Procedures:

In manual systems, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).

• Adequate Documents and Records:

In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system. In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available tot trance the transactions in a computerized system. However, if the controls over the protection and storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

• Physical Control over Assets and Records:

Physical control over access and records is critical in both manual systems and computer systems. In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster. The nature and types of control available have changed to address these new risks.

• Adequate Management Supervision:

In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location. In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried our remotely. The Management's supervision and review helps to deter and detect both errors and fraud.

• Independent Checks on Performance:

In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures. If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.

• Comparing Recorded Accountability with Assets:

Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. In a manual system, independent staff prepares the basic data used for comparison purposes. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies o the data being prepared for comparison purposes.

• Delegation of Authority and Responsibility:

A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

3.6.4 Classification on the basis of "Audit Functions"

Auditors might choose to factor systems in several different ways. Auditors have found two ways to be especially useful when conducting information systems audits. These are discussed below:

(A) Managerial Controls:

In this part, we shall examine controls over the managerial controls that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.
The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to- day basis as discussed in Table 3.6.3.

Table 3.6.3: Types of Management Subsystem and their description

Management Subsystem	Description of Subsystem
Top Management	Top management must ensure that information systems function is well managed. It is responsible primarily for long – run policy decisions on how Information Systems will be used in the organization.
Information Systems Management	IS management has overall responsibility for the planning and control of all information system activities. It also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.
Systems Development Management	Systems Development Management is responsible for the design, implementation, and maintenance of application systems
Programming Management	It is responsible for programming new system; maintain old systems and providing general systems support software.
Data Administration	Data administration is responsible for ad dressing planning and control issues in relation to use of an organization's data.
Quality Assurance Management	It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards.
Security Administration	It is responsible for access controls and physical security over the information systems function.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

(B) Application Controls:

These include the programmatic routines within the application program code. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls could include form design, source document controls, input, processing and output controls, media identification, movement and library management, data back-up and recovery, authentication and integrity, legal and regulatory requirements. Any function or activity that works to ensure the processing accuracy of the application can be considered an application control. Necessary controls belonging to this category are discussed in separate headings.

The categories of Application controls are listed below in the Table 3.6.4.

Table 3.6.4: Types of Application Subsystem and their description.

Application Subsystem	Description of Subsystem
Boundary	Comprises the components that establish the interface between the user and the system.
Input	Comprises the components that capture, prepare, and enter commands and data into the system.
Communication	Comprises the components that transmit data among subsystems and systems.
Processing	Comprises the components that perform decision making, computation, classification, ordering, and summarization of data in the system. Database Comprises the components that define, add, access, modify, and delete data in the system.
Output	Comprises the components that retrieve and present data to users of the system.

We shall study Managerial and Application Controls in detail now.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

3.7 Managerial Controls and their Categories

In this part, we shall examine controls over the managerial functions that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization. The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.

3.7.1 Top Management and Information Systems Management Controls

The senior managers who take responsibility for IS function in an organization face many challenges. The major functions that a senior manager must perform are as follows:

• **Planning –** determining the goals of the information systems function and the means of achieving these goals;

• **Organizing –** gathering, allocating, and coordinating the resources needed to accomplish the goals;

• **Leading –** motivating, guiding, and communicating with personnel; and

• **Controlling –** comparing actual performance with planned performance as a basis for taking any corrective actions that are needed.

Top management must prepare two types of information systems plans for the information systems function: a Strategic plan and an Operational plan. The strategic Plan is the long-run plan covering, say, the next three to five years of operations whereas the Operational Plan is the short-plan covering, say, next one to three years of operations. Both the plans need to be reviewed regularly and updated as the need arises. The planning depends upon factors such as the importance of existing systems, the importance of proposed information systems, and the extent to which IT has been integrated into daily operations

3.7.2 Systems Development Management Controls

Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. Three different types of audits may be conducted during system development process as discussed in the Table 3.7.1:

Table 3.7.1: Different types of Audit during System Development Process

Concurrent Audit	Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.
Post-implementation Audit	Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.

General Audit	Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements ir systems effectiveness and efficiency.

3.7.3 Programming Management Controls

Program development and implementation is a major phase within the systems development life cycle. The primary objectives of this phase are to produce or acquire and to implement high-quality programs. The program development life cycle comprises six major phases – Planning; Design; Control; Coding; Testing; and Operation and Maintenance with Control phase running in parallel for all other phases as shown in the Table 3.7.2. The purpose of the control phase during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete.

Table 3.7.2: Phases of Program Development Life Cycle

Phase	**Controls**
Planning	Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.
Coding	Programmers must choose a module implementation and integration strategy (like Top-down, bottom-up and Threads approach), a coding strategy (that follows the percepts of structured programming), and a documentation strategy (to ensure program code is easily readable and understandable).
Testing	Three types of testing can be undertaken: • Unit Testing – which focuses on individual program modules; • Integration Testing – Which focuses in groups of program modules; and • Whole-of-Program Testing – which focuses on whole program. These tests are to ensure that a developed or acquired program achieves its specified requirements.
Operation and Maintenance	Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used – Repair Maintenance – in which program errors are corrected; Adaptive Maintenance – in which the program is modified to meet changing user requirements; and Perfective Maintenance - in which the program is tuned to decrease the resource consumption.

3.7.4 Data Resource Management Controls

Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented. For data to be managed better users must be able to share data, data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed. Further it must be possible to modify data fairly easily and the integrity of the data be preserved. If data repository system is used properly, it can enhance data and application system reliability. It must be controlled carefully, however, because the consequences are serious if the data definition is compromised or destroyed. Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.

3.7.5 Quality Assurance Management Controls

Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work. Organizations are undertaking more ambitious information systems projects that require more stringent quality requirements and are becoming more concerned about their liabilities if they produce and sell defective software.

3.7.6 Security Management Controls

Information security administrators are responsible for ensuring that information systems assets are secure. Assets are secure when the expected losses that will occur over some time are at an acceptable level. Some of the major threats and to the security of information systems and their controls are as discussed in the Table 3.7.3:

Table 3.7.3: Major threats and their control measures

Threat	Control
Fire	Well-designed, reliable fire-protection systems must be implemented.
Water	Facilities must be designed and sited to mitigate losses from water damage
Energy Variations	Voltage regulators, circuit breakers, and uninterruptible power supplies can be used.
Structural Damage	Facilities must be designed to withstand structural damage.
Pollution	Regular cleaning of facilities and equipment should occur.
Unauthorized Intrusion	Physical access controls can be used.
Viruses and Worms	Controls to prevent use of virus-infected programs and to close security loopholes that allow worms to propagate.

Misuse of software, data and services	Code of conduct to govern the actions of information systems employees.
Hackers	Strong, logical access controls to mitigate losses from the activities of hackers.

3.7.7 Operations Management Controls

Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions like Computer Operations, Communications Network Control, Data Preparation and Entry, Production control, File Library; Documentation and Program Library; Help Desk/Technical support; Capacity Planning and Performance Monitoring and Outsourced Operations. Operations management control must continuously monitor the performance of the hardware/software platform to ensure that systems are executing efficiently, an acceptable response tike or turnaround time is being achieved, and an acceptable level of uptime is occurring.

Page 47

3.8.3 Communication Controls

Three major types of exposure arise in the communication subsystem:

- Transmission impairments can cause difference between the data sent and the data received;
- Data can be lost or corrupted through component failure; and
- A hostile party could seek to subvert data that is transmitted through the subsystem.

These controls discusses exposures in the communication subsystem, controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.

(A) Physical Component Controls:

These controls incorporate features that mitigate the possible effects of exposures. The Table 3.8.1 below gives an overview of how physical components can affect communication subsystem reliability.
Table 3.8.1: Physical Components affecting reliability of Communication subsystem

Transmission Media

It is a physical path along which a signal can be transmitted between a sender and a receiver. It is of two types:

- Guided/Bound Media in which the signals are transported along an enclosed physical path like – Twisted pair, coaxial cable, and optical fiber.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

• In Unguided Media, the signals propagate via free-space emission like – satellite microwave, radio frequency and infrared.

communication line.

The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.

Modem

• Increases the speed with which data can be transmitted over a Communication Line.

• Reduces the number of line errors that arise through distortion if they use a process called equalization.

• Reduces the number of line errors that arise through noise.

Port Protection Devices

• Used to mitigate exposures associated with dial-up access to a computer system. The port-protection device performs various security functions to authenticate users.

Multiplexers and Concentrators

• These allow the band width or capacity of a communication line to be used more effectively.

• These share the use of a high-cost transmission line among many messages that arrive at the multiplexer or concentration point from multiple low cost source lines.

(B) Line Error Control:

Whenever data is transmitted over a communication line, recall that it can be received in error because of attenuation distortion, or noise that occurs on the line. These errors must be detected and corrected.

• Error Detection: The errors can be detected by either using a loop (echo) check or building some form of redundancy into the message transmitted.

• Error Correction: When line errors have been detected, they must then be corrected using either forward error correcting codes or backward error correcting codes.

(C) Flow Controls:

Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data. For example, a main frame can transmit data to a microcomputer terminal. The microcomputer can not display data on its screen at the same rate the data arrives from the main frame. Moreover, the microcomputer will have limited buffer

space. Thus, it cannot continue to receive data from the mainframe and to store the data in its buffer pending display of the data on its screen. Flow controls will be used, therefore, to prevent the mainframe swamping the microcomputer and, as a result, data is lost.

(D) Link Controls:

In WANs, line error control and flow control are important functions in the component that manages the link between two nodes in a network. The link management components mainly use two common protocols HDLC (Higher Level Data Link control) and SDLC (Synchronous Data Link Control).

(E) Topological Controls:

A communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked, and the data transmission capabilities of the links between the nodes. Specifying the optimum topology for a network can be a problem of immense complexity.

• Local Area Network Topologies:

Local Area Networks tend to have three characteristics:

(1) they are privately owned networks;

(2) they provide high-speed communication among nodes; and

(3) they are confined to limited geographic areas (for example, a single floor or building or locations within a few kilometers of each other).

They are implemented using four basic types of topologies:

(1) bus topology,

(2) Tree topology,

(3) Ring topology, and

(4) Star topology.

Hybrid topologies like the star-ring topology and the star-bus topology are also used.

• Wide Area Network Topologies:

Wide Area Networks have the following characteristics:

o they often encompass components that are owned by other parties (e.g. a telephone company);

o they provide relatively low-speed communication among nodes; and

o they span large geographic areas

With the exception of the bus topology, all other topologies that are used to implement LANs can also be used to implement WANs.

(F) Channel Access Controls:

Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention for the channel exists, some type of channel access control technique must be used. These techniques fall into two classes: Polling methods and Contention methods.

• **Polling:** Polling (non contention) techniques establish an order in which a node can gain access to channel capacity.

• **Contention Methods:** Using contention methods, nodes in a network must compete with each other to gain access to a channel. Each node is given immediate right of access to the channel. Whether the node can use the channel successfully, however, depends on the actions of other nodes connected to the channel.

(G) Internetworking Controls:

Internetworking is the process of connecting two or more communication net-works together to allow the users of one network to communicate with the users of other networks. The networks connected to each other might or might not employ the same underlying hardware-software platform.
Three types of devices are used to connect sub-networks in an internet as shown in Table 3.8.3.
Table 3.8.3: Internetworking Devices.

Device	Functions
Bridge	A bridge connects similar local area networks (e.g. one token ring network to another token ring network).
Router	A router performs all the functions of a bridge. In addition, it can connect heterogeneous local are networks (e.g. a bus network to a token ring network) and direct network traffic over the fastest channel between two nodes that reside in different sub-networks (e.g. by examining traffic patterns within a network and between different networks to determine channel availability.)
Gateway	Gateways are the most complex of the three network connection devices. Their primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another. The gateway maps the functions performed in an application on one computer to the functions performed by a different application with similar functions on another computer.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

3.8.4 Processing Controls

The processing subsystem is responsible for computing, sorting, classifying, and summarizing data. Its major components are the Central Processor in which programs are executed, the real or virtual memory in which program instructions and data are stored, the operating system that manages system resources, and the application programs that execute instructions to achieve specific user requirements.

(i) Processor Controls:

The processor has three components:

(a) A Control unit, which fetches programs from memory and determines their type;

(b) An Arithmetic and Logical Unit, which performs operations; and

(c) Registers that are used to store temporary results and control information.

Four types of controls that can be used to reduce expected losses from errors and irregularities associated with Central processors are explained in the Table 3.8.4.

Table 3.8.4: Operating System Control

Control	Explanation
Error Detection and Correction	Occasionally, processors might malfunction. The causes could be design errors, manufacturing defects, damage, fatigue, electromagnetic interference, and ionizing radiation. Various types of error detection and correction strategies must be used.
Multiple Execution States	It is important to determine the number of and nature of the execution states enforced by the processor. This helps auditors to determine which user processes will be able to carry out unauthorized activities, such as gaining access to sensitive data maintained in memory regions assigned to the operating system or other user processes.
Timing Controls	An operating system might get stuck in an infinite loop. In the absence of any control, the program will retain use of processor and prevent other programs from undertaking their work.
Component Replication	In some cases, processor failure can result in significant losses. Redundant processors allow errors to be detected and corrected. If processor failure is permanent in multicomputer or multiprocessor architectures, the system might reconfigure itself to isolate the failed processor.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

(ii) Real Memory Controls:

This comprises the fixed amount of primary storage in which programs or data must reside for them to be executed or referenced by the central processor. Real memory controls seek to detect and correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access by another program.

(iii) Virtual Memory Controls:

Virtual Memory exists when the addressable storage space is larger that the available real memory space. To achieve this outcome, a control mechanism must be in place that maps virtual memory addresses into real memory addresses.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

Page 6.27

6.7 Application Controls and their Audit Trails

Application Controls and their categories have been explained in detail in Chapter 3 of the Study material. We may however again provide an overview of the same here as shown in Table 6.7.1.

Table 6.7.1: Application Controls and Audit Trail

Controls	Scope
Boundary Controls	Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.
Input Controls	Responsible for bringing both the data and instructions in to the information system. Input Controls are validation and error detection of data input into the system.
Communication Controls	Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.
Processing Controls	Responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.
Output Controls	To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.
Database Controls	Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

6.7.1 Audit Trail Controls

Two types of audit trails that should exist in each subsystem.

• An Accounting Audit Trail to maintain a record of events within the subsystem; and

• An Operations Audit Trail to maintain a record of the resource consumption associated with each event in the subsystem.

We shall now discuss Audit Trails for Application Controls in detail.

6.7.2 Boundary Controls

This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources.

• Identity of the would-be user of the system;

• Authentication information supplied;

• Resources requested;

• Action privileges requested;

• Terminal Identifier;

• Start and Finish Time;

• Number of Sign-on attempts;

• Resources provided/denied; and

Accounting Audit Trail

• Action privileges allowed/denied.

Operations Audit Trail

• Resource usage from log-on to log-out time.
• Log of Resource consumption.

6.7.3 Input Controls

This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.

Accounting Audit Trail

• The identity of the person(organization) who was the source of the data;

• The identity of the person(organization) who entered the data into the system;

• The time and date when the data was captured;

• The identifier of the physical device used to enter the data into the system;

• The account or record to be updated by the transaction;

• The standing data to be updated by the transaction;

• The details of the transaction; and

• The number of the physical or logical batch to which the transaction belongs.

Operations Audit Trail

• Time to key in a source document or an instrument at a terminal;

• Number of read errors made by an optical scanning device;

• Number of keying errors identified during verification;

• Frequency with which an instruction in a command language is used; and

• Time taken to invoke an instruction using a light pen versus a mouse.

6.7.4 Communication Controls

This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.

Accounting Audit Trail

• Unique identifier of the source/sink node;

• Unique identifier of each node in the network that traverses the message; Unique identifier of the person or process authorizing dispatch of the message; Time and date at which the message was dispatched;

• Time and date at which the message was received by the sink node;

• Time and date at which node in the network was traversed by the message; and

• Message sequence number; and the image of the message received at each node traversed in the network.

Operations Audit Trail

• Number of messages that have traversed each link and each node;

• Queue lengths at each node; Number of errors occurring on each link or at each node; Number of retransmissions that have occurred across each link; Log of errors to identify locations and patterns of errors;

• Log of system restarts; and

• Message transit times between nodes and at nodes.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

6.7.5 Processing Controls

The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.

Accounting Audit Trail

• To trace and replicate the processing performed on a data item.

• Triggered transactions to monitor input data entry, intermediate results and output data values.

Operations Audit Trail

• A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used.

• A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

6.7.5 Database Controls

The audit trail maintains the chronology of events that occur either to the database definition or the database itself.

Accounting Audit Trail

• To attach a unique time stamp to all transactions,

• To attach before images and afterimages of the data item on which a transaction is applied to the audit trail; and

• Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.

Operations Audit Trail

• To maintain a chronology of resource consumption events that affects the database definition or the database.

6.7.6 Output Controls

The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.

Accounting Audit Trail

• What output was presented to users;

- Who received the output;
- When the output was received; and
- What actions were taken with the output?

Operations Audit Trail

- To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

Chap 7

Page 7.39

ISO 27001

How the standard works?

ISO 27001 requires that management:

- systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

History

ISO/IEC 27001 is derived from The British Standard BS 7799 Part 2, published in 1999. BS 7799 Part 2 was revised by BSI in 2002, explicitly incorporating Deming's PDCA process concept, and was adopted by ISO/IEC as ISO/IEC 27001 in 2005. It was extensively revised in 2013, bringing it into line with the other ISO certified management systems standards and dropping the PDCA concept.

(a) ISO/IEC 27001:2005, part of the growing ISO/IEC 27000 family of standards, was an Information Security Management System (ISMS) standard published in October 2005 by ISO/IEC. Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information Security Management Systems – Requirements. It was superseded, in 2013, by ISO/IEC 27001:2013.

The Plan-Do-Check-Act (PDCA) cycle

ISO 27001 prescribes 'How to manage information security through a system of information security management'. Such a management system consists of four phases that should be continuously implemented in order to minimize risks to the Confidentiality, Integrity and Availability (CIA) of information.

The PDCA cyclic process is shown in the Fig. 7.13.1 and is explained below:

- **The Plan Phase (Establishing the ISMS) –**

This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).

- **The Do Phase (Implementing and Working of ISMS) –**

This phase includes carrying out everything that was planned during the previous phase.

- **The Check Phase (Monitoring and Review of the ISMS) –**

The purpose of this phase is to monitor the functioning of the ISMS through various “channels”, and check whether the results meet the set objectives.

- **The Act Phase (Update and Improvement of the ISMS) –**

The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The cycle of these four phases never ends, and all the activities must be implemented cyclically in order to keep the ISMS effective. ISO/IEC 27001:2005 applies this to all the processes in ISMS.

(b) ISO/IEC 27001:2013

is the first revision of ISO/IEC 27001 that specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System within the context of the organization. It is an information security standard that was published on 25th September 2013. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. ISO 27001:2013 does not put so much emphasis on this cycle.

Structure

In the new structure, the Processing Approach, used in ISO27001:2005, and which houses the PDCA model, was eliminated. The reason for this is that the requirement is for continual improvement and PDCA is just one approach to meeting that requirement. There are other approaches, and organizations are now free to use them if they wish. The introduction also draws attention to the order in which requirements are presented, stating that the order does not reflect their importance or imply the order in which they are to be implemented.

27001:2013 has ten short clauses, plus a long Annex, which covers the following:

Clause 1: Scope

Clause 2: Normative references

Clause 3: Terms and Definitions

Clause 4: Context of the organization

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

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 114 controls in 14 groups (A.5 to A.18), in contrast to 133 controls in 11 groups in the old standard.

A brief mention about the groups and their controls are mentioned below:

- A.5: Information security policy (2 controls)
- A.6: Organization of information security (7 controls)
- A.7: Human resource security (6 controls that are applied before, during, or after employment)
- A.8: Asset management (10 controls)
- A.9: Access control (14 controls)
- A.10: Cryptography (2 controls)
- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls)
- A.13: Communications security (7controls)
- A.14: Information systems acquisition, development and maintenance (13 controls)
- A.15: Relationship with external parties (5 controls)
- A.16: Information security incident management (7 controls)
- A.17: Information security in business continuity management (4 controls)
- A.18: Compliance with legal and contractual requirements (8 controls)

Changes from the 2005 standard

The new standard puts more emphasis on measuring and evaluating how well an organization's ISMS is performing, and there is a new section on outsourcing, which reflects the fact that many organizations rely on third parties to provide some aspects of IT. It does not emphasize the PDCA cycle that 27001:2005 did. Other continuous improvement processes like Six Sigma's DMAIC method can be implemented. More attention is paid to the organizational context of information security, and risk assessment has changed. Overall, 27001:2013 is designed to fit better alongside other management standards such as ISO 9000 and ISO 20000, and it has more in common with them.

A couple of the major changes to the standard are:

• Annex A has been revised and restructured; there are now 114 controls under 14 categories rather than the previous 133 controls under 11 categories.

• The Plan-Do-Check-Act Cycle (PDCA) is no longer mandated.

Page 7.43

7.13.3 Information Technology Infrastructure Library (ITIL)

The IT Infrastructure Library (ITIL) is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

Although the UK Government originally created the ITIL, it has rapidly been adopted across the world as the standard for best practice in the provision of information technology services. As IT services become more closely aligned and integrated with the business, ITIL assists in establishing a business management approach and discipline to IT Service Management, stressing the complementary aspects of running IT like a business. Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services. The core of Service Management is transforming resources into valuable services.

ITIL V3 represents an important change in best practice approach, transforming ITIL from providing a good service to being the most innovative and best in class. At the same time, the interface between old and new approaches is seamless, making adoption simple for those experienced in ITIL V2. ITIL V3 makes the link between ITIL's best practice and business benefits both clearer and stronger. Based on a core of five titles, the changes in ITIL V3 reflect the way IT Service Management has matured over the past decades and change the relationship between IT and business. Whereas previously ITIL worked to align Service Management with business strategy, ITIL V3 integrates into a single lifecycle, and well depicted in Fig. 7.13.2.

This release of ITIL V3 brought with it an important change of emphasis, from an operationally focused set of processes to a mature service management set of practice guidance. It also brought a rationalization in the number of volumes included in the set.

• **Service Strategy:** This provides guidance on clarification and prioritization of service- provider investments in services;

• **Service Design:** This provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort;

• **Service Transition:** This elates to the delivery of services required by a business into live/operational use, and often encompasses the "project" side of IT rather than Business As

Usual (BAU);

• **Service Operation:** This provides best practice for achieving the delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the SLAs), and

• **Continual Service Improvement:** This aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes.

Details of the ITIL Framework: Details of these aforementioned volumes are given as follows:

I. Service Strategy:

The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service- provider investments in services. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers. The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset. It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

• **IT Service Generation:** IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process and Information Technology.

• **Service Portfolio Management**: IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.

• **Financial Management:** Financial Management for IT Services' aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.

• **Demand Management:** Demand management is a planning methodology used to manage and forecast the demand of products and services.

• **Business Relationship Management:** Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services via networks.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

II. Service Design:

Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.
The Service Design volume provides guidance on the design and development of services and service management processes. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets. Service Design is not limited to new services and includes the changes and improvements required to maintain or increase value to customers over the lifecycle of services, taking into account the continuity of services, conformance to standards and regulations and achievement of service levels. It also provides guidance on the development of design capabilities for service management.

• Service Catalogue Management:

Service Catalogue management maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers. Service Catalogue information includes ordering and requesting processes, prices, deliverables and contract points.

• Service Level Management:

Service-level management provides for continual identification, monitoring and review of the levels of IT services specified in the Service-Level Agreements (SLAs). Service-Level Management is the primary interface with the customer and is responsible for ensuring that the agreed IT services are delivered when and where they are supposed to be; liaising with availability management, capacity management, incident management and problem management.

• Availability Management:

Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost. The high-level activities comprise of realizing availability requirements, compiling availability plan, monitoring availability and maintenance obligations. Availability management addresses many IT component abilities like reliability, maintainability, serviceability, resilience and security to perform at an agreed level over a period of time.

• Capacity Management:

Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands. The high-level activities include application sizing; workload management; demand management; modelling; capacity planning; resource management and performance management.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

• IT Service Continuity Management:

IT Service Continuity Management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs.

• Information Security Management:

A basic goal of security management is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their confidentiality, integrity and availability, along with related properties or goals such as authenticity, accountability, non-repudiation and reliability.

• Supplier Management:

The purpose of Supplier Management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements. Supplier Management oversees process of identification of business needs, evaluation of suppliers, establishing contracts, their categorization, management and termination.

III. Service Transition:

Service Transition provides guidance on the service design and implementation ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively. Service Transition planning provides guidance on managing the complexity of changes to services and service management processes to prevent undesired consequences whilst permitting for innovation. It provides guidance on the support mechanism on transferring the control of services between customers and service providers. The Service Transition volume provides guidance on the development and improvement of capabilities for transitioning new and changed services into operations. Guidance is provided on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation, whilst controlling the risks of failure and disruption. It combines the processes in Release, Program and Risk Management and sets them in the practical context of Service Management.

• Service Transition Planning and Support:

The service transition planning and support process ensures the orderly transition of a new or modified service into production, together with the necessary adaptations to the service management processes. The service transition planning and support process must incorporate the service design and operational requirements within the transition planning.

• Change management and Evaluation:

This aims to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is an event that results in a new status of one or more configuration items

(CIs), and which is approved by management, is cost-effective, enhances business process changes (fixes) – all with a minimum risk to IT infrastructure.

• Service Asset and Configuration Management:

Service Asset and Configuration Management is primarily focused on maintaining information (i.e., configurations) about Configuration Items (i.e., assets) required to deliver an IT service, including their relationships. Configuration management is the management and traceability of every aspect of a configuration from beginning to end.

• Release and Deployment Management:

Release and deployment management is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper software and hardware control ensures the availability of licensed, tested, and version-certified software and hardware, which functions as intended when introduced into existing infrastructure.

• Service Validation and Testing:

The objective of ITIL Service Validation and Testing is to ensure that deployed Releases and the resulting services meet customer expectations, and to verify that IT operations are able to support the new service.

• Knowledge Management:

Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organisational knowledge. It refers to a multi-disciplined approach to achieving organisational objectives by making the best use of knowledge.

IV. Service Operation:

Service Operation provides guidance on the management of a service through its day-to-day production life. It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

• Functions:

The major functions are as follows:

o Service Desk: The service desk is one of four ITIL functions and is primarily associated with the Service Operation lifecycle stage. Tasks include handling incidents and requests, and providing an interface for other ITSM processes. Features include Single Point of Contact (SPOC); Single Point of Entry and Exit; easier for customers and streamlined communication channel.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com

o Application management: ITIL application management encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.

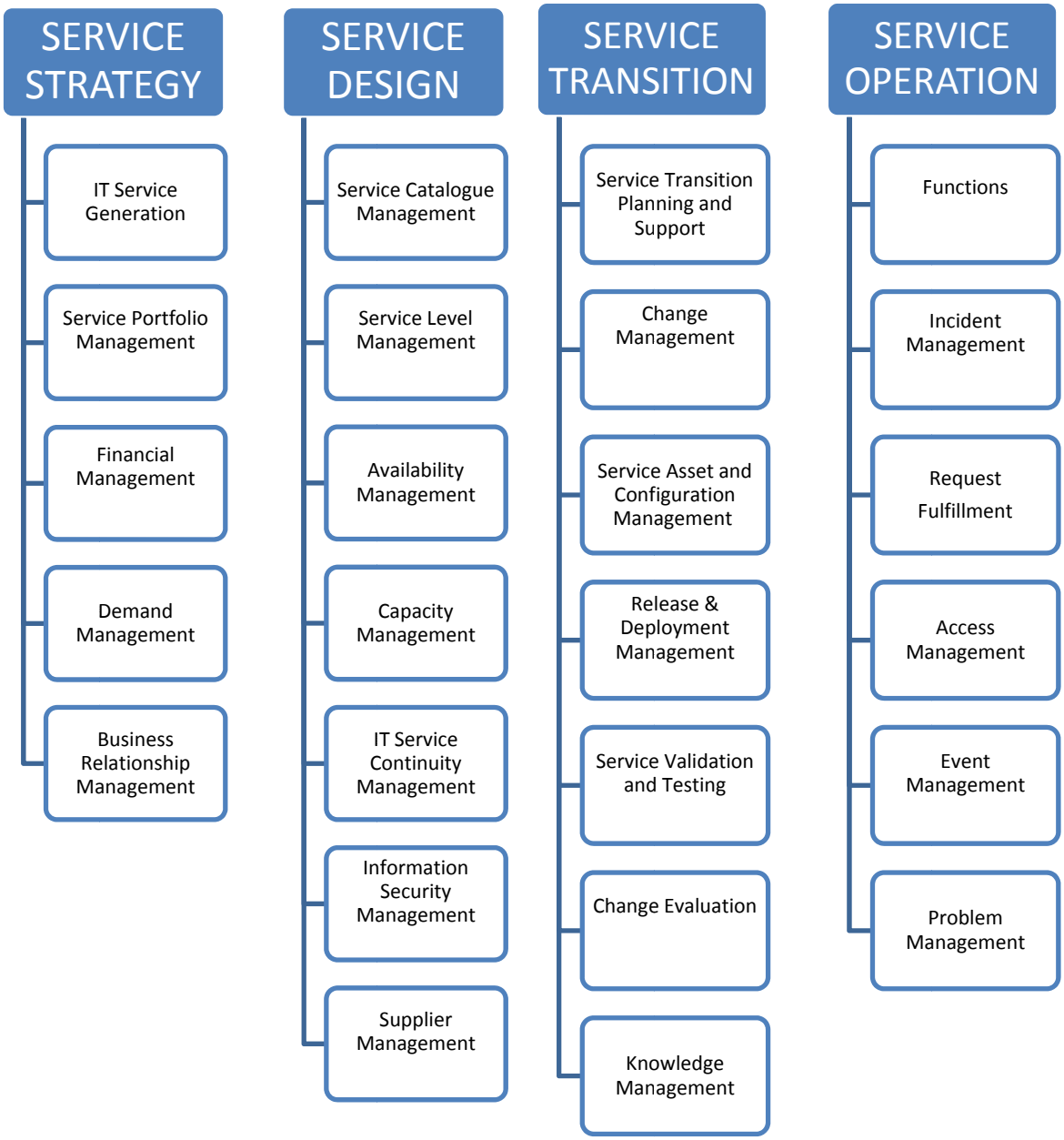
o IT Operations: IT Operations primarily work from documented processes and procedures and should be concerned with a number of specific sub-processes, such as: output management, job scheduling, backup and restore, network monitoring/management, system monitoring/ management, database monitoring/management storage monitoring/management.

o IT Technical Support: IT technical support provides a number of specialist functions: research and evaluation, market intelligence, proof of concept and pilot engineering, specialist technical expertise, and creation of documentation.

• **Incident Management:** Incident management aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.
• **Request fulfillment:** Request fulfillment (or request management) focuses on fulfilling Service Requests, which are often minor changes (e.g., requests to change a password) or requests for information.

Event Management: An event may indicate that something is not functioning correctly, leading to an incident being logged. Event management generates and detects notifications, while monitoring checks the status of components even when no events are occurring.

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com



Continual Service Improvement Fig. 7.13.2: ITIL V3

Prepared By: Dimple Hirapara
dimpypatel9757@gmail.com