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.

1.10.4 Benefits of COBIT 5: COBIT 5 framework 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.

The COBIT 5 process reference model is the successor of the COBIT 4.1 process model, incorporating the both the Risk IT and Val It frameworks. The complete COBIT 5 enabler model includes a total of 37 governance and management processes as mentioned below:

- Governance Processes
- Evaluate, direct and Monitor Practices (EDM) – 5 processes (EDM 01 to EDM 05)
- Management Processes
- Align, Plan and Organize (APO). 13 processes (APO 01 to APO13)

- Build, Acquire and implement (BAI)-10 processes (BAI 01 to BAI 10)
- Deliver, Service and Support (DSS)-6 processes (DSS 01 to DSS 06)
- Monitor, evaluate and Assess (MEA). 3 processes (MEA 01 to MEA 03)

(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. 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). Knowledge Management (KM) is the process of capturing, developing sharing, and effectively using organizational objectives by making the best use of knowledge. Knowledge Management System (KMS) refers to any kind of IT system that stores and retrieves knowledge, improves collaboration, locates knowledges sources, mines repositories for hidden knowledge, captures and uses knowledge, or in some other way enhances the KM process.

There are two broad types of knowledge- Explicit and Tacit as shown in the Fig. 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 captures by the organization or made available to other. 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.

(B) Cross Functional Information Systems: 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.

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 illustrate 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 towards 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.
- Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.
- Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.
- Track actual costs of activities and perform activity based costing.
- 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 function will include transaction accounts, loans, mortgages and payments. Banks make these services available across multiple channels like ATMs, Internet banking, and branches.

These systems typically include deposit, loan and credit processing capabilities, with interfaces to general ledger systems and reporting tools. Examples of core banking products include Infosys' Finacle, Nucleus Finn One and Oracle's Flexcube application. 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.

3.5.4 Impact of Technology on Internal Controls

These are discussed as follows:

- **Component and Trustworthy Personnel:** Personnel should have proper skill and knowledge to discharge their duties. Substantial power often results in the errors. Therefore, it is difficult to find component and trustworthy information system personnel.
- **Segregation of Duties:** In a manual system, processing of a transaction are spread between 2 or more people, such that one person does not process a transaction right from start to finish. Similarly, in a computerised system, the auditor should be concerned with the segregation of duties within the IT department which would prevent or detect errors or irregularities.

- **Authorization Procedures:** In manual systems, auditor evaluates the procedure of authorization for examining the work of employees. However, in computer systems, authorization procedures often are embedded within a computer program.
- **Adequate Documents and Records:** In a manual system, adequate documents and records are needed to provide an audit trial of activities within the system. However, in computer systems, documents might not be used to support the process of transactions and therefore no visible audit or management trail would be available. However, if the controls over the storage of documents, transaction etc. are placed properly, it will not be a problem for auditor.
- **Physical Control over Assets and Records:** In manual systems, protection from unauthorized access was through the use of locked doors and filing cabinets. However, the needs to protect the data in computerised financial system have still not changed. A client's financial data are stored at a single site where computer is located and therefore any kind of computer abuse or a disaster would results in heavy losses.
- **Adequate Management Supervision:** In a manual system, management supervision is quite easy as the managers and the employees are often at the same physical location. However, in computer system, data communication facilities can be used to enables employees to be closed to their customers. 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. However, if program code in a computer system is properly authorized, accurate, and complete, then the system will always follow the designed procedure.
- **Comparing recorded accountability with Assets:** Data and the assets both should be periodically compared to determine whether any inaccuracies in the data exist or whether any 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, software is used to prepare this data.
- **Delegation of Authority and Responsibility:** There should be clear line of authority and responsibility in both manual and computer systems. However, in a computer system it would be difficult to delegate authority unambiguous because same resources are shared among multiple users.

3.5.4 Classification on the basis of "Audit Functions":

Classification on the basis of Audit Function can be done in following ways:

(A) Managerial Controls: Here, managerial controls are examined to ensure that the development, operation and maintenance of information systems are carried out in a planned and controlled manner. Types of management subsystem and their description are as follows:

- **Top Management:** Top management are primarily responsible for long – run policy decisions on how Information Systems will be used in the organization and must also ensure they are well managed.
- **Information System Management:** They have the overall responsibility for the planning and control of all information system activities. Further they also provide 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:** They are responsible for the design, implementation, and maintenance of application systems.
- **Programming Management:** They are responsible for programming new system; maintain old systems and providing general system support software.
- **Data Administration:** They are responsible for planning and control issues in relation to proper usage of an organisation's data.
- **Quality Assurance Management:** They must ensure that the information system s development; operation, and maintenance conform to established quality standards.
- **Security Administration:** They are responsible for access control and physical security for information system function.
- **Operations Management:** They are responsible for planning and control of the day to day operations of information systems.

(B) Application Controls: The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage stage. Any function or activity that works ensure processing accuracy of the application can be considered as an application control.

The categories of Application controls and their description are as follows:

- **Boundary:** They establish the interface between the user and the system.
- **Input:** they capture, prepare, and enter commands and data into the system.
- **Communication:** They transmit data among subsystems and systems.
- **Processing:** They perform decision making, computation, classification, ordering, and summarization of data in the system.
- **Database:** They define, add access, modify, and delete data in the system.

- **Output:** They retrieve and present data to users of the system.

3.6 Managerial Controls and their Categories

Managerial controls must ensure the development, implementation, operation and maintenance of information systems are carried out in a planned and controlled manner. The controls at this level provide a stable infrastructure for information systems to build, operate and maintain on a day to day basis.

3.6.1 Top Management and Information Systems Management Controls.

The major function that a senior manager must perform for IS functioning in an organization are as follows:

- **Planning:** It means determining the goals of the IS function and the means of achieving these goals;
- **Organizing:** It means gathering, allocating, and coordinating the resources which are needed to accomplish the goals;
- **Leading:** It means motivating, guiding, and communicating with personnel; and
- **Controlling:** It compares actual performance with the planned performance so that corrective actions can be taken, if required.
- Top management must prepare two types of plans for the information systems function: a Strategic plan and an Operational plan. The strategic Plan is the long run plan covering, for next three to five years of Operational plan. The Strategic Plan is the long run plan covering, for next three to five years of operations whereas the Operational Plan is the short-plan covering, for one to three years of operations.
- Both the plans need should be reviewed regularly and updated as and when required.

3.6.2 Systems Development Management Controls

They are concerned with analyzing, designing, building, implementing, and maintaining information systems. Three different types of audits may be concluded during system development process are as follows:

- **Concurrent Audit:** Here auditors are member of the system development team and assists the team in improving the quality of systems development.
- **Post implementation Audit:** Here auditor's helps organization from his own experience obtained during development stage. Further, they might also be evaluating whether the system needs to be scrapped, continued, or modified in some way.
- **General Audit:** Here auditors evaluate overall systems development controls. 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 in systems effectiveness and efficiency.

3.6.3 Programming Management Controls

The primary objective of this phase is to produce or acquire and implement high quality programs. The program development life cycle comprises six major phases- Planning; Design; Control; Coding; Testing; and Operation and Maintenance. The purpose of the control phase during software development or acquisition is to monitor progress against the plan and to ensure that software released for production is authentic, accurate, and complete.

- **Planning:** Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Chart can be used to monitor progress against plan.
- **Design:** A systematic approach to program design in the form of structured design or object oriented design should be 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 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 program modules; and
    - Whole of Program Testing which focuses on whole program.

    These tests ensure that a developed or acquired program achieves its specified requirements.

- **Operation and Maintenance:** Management monitor the status of operational programs so that 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 programs are modified to meet changing user requirements; and
    - Perfective Maintenance- in which the programs are tuned to decrease the resource consumption.

3.6.4 Data Resource Management Controls

Today data is a critical resource which must be managed properly and therefore, centralized planning and control should be implemented. Data can be managed better, if users are able to share data, data must be available to users as and when needed. Further it must be possible to modify data easily and the integrity of data is also preserved. Careful control should be exercised over the roles by appointing senior, separating duties to the extent possible and security of data because consequences are serious if data is compromised or destroyed.

3.6.5 Quality Assurance Management Controls

Organizations are increasingly producing safety critical systems and users are also becoming more demanding in terms of the quality of the software they work with. Organizations are undertaken more ambitious information systems projects which require more stringent quality requirements and are also becoming more concerned about their liabilities if they produce and sell defective software.

3.6.6 Security Management Controls

Information security administrators are responsible to ensure that information systems assets are secure. Assets are secure when the expected losses are at an acceptable level. Some of the major threats to the security of information systems and their controls are discussed as follows:

- **Fire:** Well –designed, reliable fire protection system 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 control can be used.
- **Viruses and Worms:** Control should be implemented to prevent use of virus – infected programs and to close security loopholes that allow worms to reproduce itself.
- **Misuse of software, data and services:** Code of conduct to govern the actions of information systems employees.
- **Hackers:** Strong logical access controls should be implemented to mitigate losses from the activities of hackers.

3.6.7 Operations Management Controls

Operations Management is responsible for the daily running of hardware and software facilities to ensure that systems are executing efficiently, an acceptable response like or turnaround time is being achieved, and an acceptable level of uptime is occurring. They typically performs controls over the functions like Computer Operations, Data Preparation and Entry, Production control, File Library; Documentation and Program Library; Help Desk/ Technical Support; etc.

3.7 Application Controls and their Categories

Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions. Different Application Controls are as follows:

3.7.1 Boundary Controls

(i) Boundary Controls: [means how user will enter into the system]: Boundary systems deals with access over the system. Access controls links the users to resources who are permitted to access those resources through three step identification, authentication and authorization through which user can access the required resources.

6.6 Application Controls and their Audits Trails

Application Controls and their categories have been explained in details 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

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, flow, 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 contents available to users, data format, timelineness 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.

6.6.1 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.

6.6.2 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.

6.6.3 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 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.

6.6.4 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 length at each node; Number of errors occurring on each link or at each node; Number of retransmission 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.

6.6.5 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- compliers used, subordinate libraries used, file management facilities used, and communicate software used.

6.6.6 Database Controls

The audit trial maintains the chronology of events that occur either to the database definitions 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 trial; and Any modifications or correction to audit trial transactions accommodating the changes that occur within an application system.

Operations Audit Trial

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

6.6.7 Output Controls

The audit trial maintains the chronology of events that occurs 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?

7.11.1 ISO 27001: ISO 27001 is the international best practice and standard for an information Security Management System (ISMS). An ISMS is a systematic approach for managing confidential information so that it remains secure. It encompasses people, processes and IT systems.

ISO 27001 defines how to organize information security in any kind of organization and therefore different security should be prioritized to ensure overall effectiveness. ISO 27001 is for information security; the same thing that ISO 9001 is for quality.
Today ISO 27001 is being taken as a basis for drawing up different regulation in various fields like personal data protection, protection of confidential information, protection of information systems, etc.

How the standards 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. and is explained below:

Fig

These phases are given as follows:

- **The Plan Phase (Establishing the ISMS):** This phase plans basic requirement of information security, set objectives for information security and choose the appropriate security controls accordingly.
- **The Do Phase (Implementing & working of ISMS):** This phase carries out activity that was planned in the previous phase.

- **The Check Phase (Monitoring & review of ISMS):** This phase monitors the functioning of the ISMS through various "Channels", and check whether the results meet the set objectives.
- **The Act Phase (Update & Improvement of ISMS):** The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The details description of all these above mentioned phases is given as follows:

(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 risk 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
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation
- Clause 10: Improvement

Annex A: List of controls on 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 (7 controls)
- A.14: Information system 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 outstanding, 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.

(2) Other Related Aspects: ISO 27001 requires that management:

- Systematically examines the organization's information security risks, threats and vulnerabilities along with their impacts;
- Design and implement comprehensive information security controls and/or other forms of risk treatment(such as risk avoidance or risk transfer) to address those risk that are deemed unacceptable; and
- Adopt management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

7.11.3 ITIL (IT Infrastructure Library): The Information Technology Infrastructure Library (ITIL) is a set of practices for IT Service Management (ITSM) which focusses on aligning IT services with business needs. ITIL is published in a series of five core publication in its current form which describes procedures, tasks and checklists those are not organization-specific for establishing a minimum level of competency. It also allows organization to establish a baseline from which it can plan, implement, and measure.

Today, IT services are more closely aligned and integrated with the business and therefore ITIL assists in establishing a business management approach and disciplines to IT Service Management by providing value to customers in the form of services. The core of Service Management is transforming resources into valuable services.

The 5 phases of ITIL are as follows:

- Service Strategy,
- Service Design,
- Service Transition,
- Service Operation, and
- Continual Service Improvement.

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

Service Strategy: Service Strategy deals with the strategic management approach in respect of IT Service Management as well as strategic analysis, planning and implementation of service models, strategies, and strategic objectives. It provides guidance on how to improve service management capabilities to effectively deliver value to the customers and also illustrate value for service providers.

- **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 Service' 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.
- **Service Design:** Service Design translates strategic plans and objectives and creates the designs and specifications as per requirements for execution through service operations. It provides best feasible combination of infrastructure, applications, systems, and processes, along with suppliers for service offerings.
- **Service Catalogue Management:** Service catalogue management maintains and procedures 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. 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.

- **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.
- Suppliers 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.
- **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 Transaction provides guidance on managing the complexity of changes to services and processes to events undesired consequences whilst permitting for innovation. It also provides guidance on transferring the control of services between customers and service providers.
- **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 9CIs), 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 aspects 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 organizational knowledge. It refers to a multi-disciplined approach to achieving organizational objectives by making the best use of knowledge.
- **Service Operation:** Service Operation provides guidance on the management of a service for its day to day operation as well as for supporting operations through new models like shared services, web services mobile commerce, etc.
  Service Operation provides detailed guidelines on processes, methods and tools in addressing the proactive and reactive control perspectives. Managers are provided with knowledge to enable them to make better informed decisions in areas such as managing the availability of services, optimizing capacity utilization, fixing problems, etc.
- **Functions: The major functions are as follows:**
  - **Service Desk:** The service desk is one of four ITIL functions and is primarily associated with the Service Operation lifecycle stage. Task include handling incidents and requests, and providing an interface for other ITSM processes. Features include Single Point of Contract (SPOC); Single Point of Entry and Exit; easier for customers and streamlined communication channel.
  - **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.
  - **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.
  - **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 fulfilment:** Request fulfilment (or request management) focuses on fulfilling Service requests, which are often minor changes (e.g., request to change a password) or request 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.
- **Continual Service Improvement:** Continual Service Improvement measures the service performance through service life-cycle and suggests improvements to ensure that a service delivers the maximum benefit. It combines methods from change management, quality management, and capability improvement to achieve significant improvements in service quality and business continuity.

PAGE NO- 1.4

Regulatory requirements and standards generally address this dimension; however, compliance being subject to audit. There are also mechanisms to ensure that good corporate governance processes are effective and these include committees comprising of independent non-executive directors, particularly the audit committee or its equivalent. The Sarbanes Oxley Act of US and Clause 49 listing requirements of SEBI are examples of providing for such compliances from conformance perspective.

Good corporate governance is important and also critical so that any weakness can be addressed properly. However, good corporate governance, itself cannot make an organization successful because there is always a risk that enterprise might pay inadequate attention to the need of wealth creation or stakeholder value. Therefore, the key message of enterprise governance is that an enterprise must balance both the two dimensions of conformance and performance so as to meet stakeholder requirements and also ensure long-term success.

- **Performance or Business Governance Dimension:** The performance dimension is proactive in its approach. It focusses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. However, this dimension is not governed by any standards as this is specific to enterprise goals. It is advisable to develop appropriate best practices and techniques such as balanced scorecards and strategic enterprise system that can be applied intelligently for different types of enterprises as required.
  Comparison: The conformance dimension is monitored by the audit committee. However, the performance dimension is the responsibility of the full board but there is no dedicated mechanism as comparable to the audit committee. Remuneration and financial reporting of conformance dimension are scrutinized by a specialist board committee and referred back to board. In contrast, the critical area of strategy of performance dimension does not get the same dedicated attention. Thus, there is an oversight gap in respect of strategy. This can be dealt by establishing a strategy committee of similar status as of board committees which will report to the board.

PAGE NO-1.18

1.10.2 Integrating COBIT 5 with Other Frameworks: COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance. COBIT 5 provides basis to integrate other frameworks, standards and practices used such as ITIL, TOGAF and ISO 27001 effectively. It is also aligned with. The GEIT standard which has set high level principles for the governance of IT which governing body (i.e., board) should evaluate in the form of responsibility, strategy acquisition, performance, compliance and human behavior. Thus, COBIT 5 acts as the single overarching framework, which serves as a integrated source of guidance for other framework which should be aligned with the:

- Enterprise policies, strategies, governance and business plans, and audit approaches;
- Enterprise risk management framework; and
- Existing enterprise governance organization, structures and processes.

PAGE NO-1.20

1.10.7 COBIT 5 Process Reference Model: COBIT 5 includes a Process reference Model, which defines and describes in detail a number of governance and management processes of enterprise IT into two main process domains-Governance and Management as shown in Fig 1.10.3. It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference modal understandable to operational IT and business managers. The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must defines its own process set, taking into account its specific situation.

Incorporating an operational model and a common language for all parts of the enterprise involved in IT activities is one of the most important and critical steps towards good governance, it also provides a framework for measuring and monitoring IT performance, providing IT assurance, communicating with service providers, and integrating best management practices.

- **Governance:** Ensures that stakeholder needs are evaluated, enterprise objectives to be achieved; setting direction through prioritization and decision-making; and monitoring performance against set direction and objectives. In most enterprises, overall governance is the responsibility of the board of directors.
- **Management:** Management plans and monitors whether activities are in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management.

PAGE NO-1.3

The enterprise governance constitutes the entire accountability framework of an organization as it involves establishing accountability for decision making.

Governance has two dimensions:

- Conformance or Corporate Governance; and
- Performance or Business Governance.

PAGE NO-1.16

Countermeasure: An action, technique or any other measures that reduces the vulnerability of a system is referred as countermeasure. For examples, 'spoofing the user identity threat can be prevented through two countermeasures:

- By inserting strong authentication protocols to validate users; and
- By storing passwords through secure mechanism and not in configuration files.

Similarly, for other vulnerabilities, different countermeasures may be used.

PAGE NO-2.7

Knowledge – Level Systems: These system support discovery, processing and storage of knowledge and data workers. These support the business to integrate new knowledge into the business and control the flow of paperwork and enable group working.

PAGE NO-2.14

Strategic Level Systems: It supports the senior level management to tackle and address strategic issues and long term trends. It answer questions like what products should be launched to increase the profit and capture the market.

PAGE NO- 2.16

SPECIALISED SYSTEMS: There are also various other categories of information systems which supports either operations or management applications. These are Expert Systems, Knowledge Management Systems, Functional Business Information Systems, Strategic Information Systems and Cross Functional Information Systems. These are discussed one by one as follows:

PAGE NO-3.27

3.7.2 Input Controls: They are responsible for accuracy and completeness of data and instruction input into an application system. Input control is important because substantial amount of time is spent on input of data which involves human intervention and are therefore prone to error or fraud. The auditor should therefore evaluate the coding Systems.

Existence/Recovery Controls: Controls relating to input data are critical. It might be necessary to reprocess input data when master files are lost or destroyed. Thus, source documents are to be stored securely for longer periods and also for statutory requirements as well.

PAGE NO-3.28

(C) Batch Controls: Batching is the process of grouping transactions together that has some type of relationship with each other. Various controls can be exercises over the batch to prevent or detect errors or irregularities. Two types of batches occur:

- **Physical Control:** These control are groups of transactions that constitute a physical unit. For example-source documents might be obtained via the email, assembled into batches, grouped and tied together, and then given to a data-entry clerk to be entered into an application system at a terminal.
- **Logical Controls:** These are group of transactions bound together on some logical basis, rather than being physically connected. For example-different clerks might use the same terminal to enter transaction into an application system.
  To identify errors or irregularities in either a physical or logical batch, three types of control totals can be calculated as shown in Table:

Control Total Type	**Explanation**
Financial Totals	Grand totals calculated for each field containing money amounts.
Harsh Totals	Grand totals calculated for any code on a document in the batch, eg., the source document serial numbers can be totaled.

Document/Record Counts	Grand totals for the number of documents in record in the batch.

- In case of Physical Controls, these totals can be written on the batch cover sheet and entered into the application system prior to the key entry of the transaction in the batch. Now, the input program computes the batch to the key entry of the transactions are entered. When all the transactions in the batch have been completed, it compares the computed total against the written total and signals any discrepancy.
- In case of logical batch, the person responsible for entering data must keep an independent record of transactions entered into the application system. Periodically, the batch totals calculated by the input program must be compared against the batch totals of these independent records.

PAGE NO-3.30

3.7.3 Communication Controls

Three major types of exposure arise in the communication subsystem:

- Transmission damage can cause difference between the data sent and the data received;
- Data can be lost or corrupted through component (i.e., part) failure; and
- A hostile party could seek to weak data that is transmitted through the subsystem.

Following controls can be implemented in case of communication subsystems:

(a) Physical Component Controls: These controls mitigate the possible effects of exposures. Physical Components affecting reliability of Communication subsystems are as follows:
- **Transmission Media:** It is physical path along which a signal can be transmitted between a sender and a receiver. It is of two types:
- **Guided/Bound Media:** Here signals are transported through physical path like-Twisted pair, coaxial cable, and optical fiber.
- **In Unguided Media:** Here, signals propagate via free-space emission like-satellite microwave, radio frequency and infrared.
- **Communication Lines:** The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.

- **Modem:** Increase the speed with which data can be transmitted over a communication line. Reduces the number of line errors that arise through noise.
- **Port Protection Devices:** They are used to mitigate exposures associates with dial-up access through security function to authenticate users to a computer system.
- **Multiplexers and Concentrators:** They allow the band width or capacity of a communication line to be used more effectively.
  They 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, it can be received in error because of attenuation distortion, or noise 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 (program) in a network can differ in terms of the rate at which they can send, received, and process data. For example, main frame transmit data to a microcomputer. However microcomputer cannot display data on its screen at the same rate at which data is arriving from the main frame. Further, microcomputer has limited buffer space. Thus, as a result it cannot continue to receive the data from the mainframe and also cannot store the data in its buffer space. Therefore, flow controls should be used so that the mainframe controls the flow of transmission of data to microcomputer and thus preventing data from being lost.

(d) Link Controls: In WANs, line error control and flow control are important function 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: It specifies the location of nodes within a network, the ways in which nodes will be linked, and the data transmission capabilities of the links between the nodes.

- **Local Area Network Topologies:** Local Area Network 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 area within a few kilometers). They are implemented using four 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 Network have the following characteristics:
  - they often include components that are owned by other parties (e.g. a telephone company);
  - they provide relatively low-speed communication among nodes; and
  - they span large geographic areas

  They are implemented using 3 types of topologies: (1) Tree topology, (2) Ring topology, and (3) Star topology.

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

- **Polling:** It establishes an order (i.e., sequence) in which a node can gain access to channel capacity.
- **Contention Methods:** Here, nodes in a network must complete with each other to gain access to a channel. However, whether the node can use the channel successfully 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. Three types of devices are used to connect sub-networks in an internet which are as follows:
Bridge: A bridge connects similar local area networks (e.g. one token ring networks to another token ring network).
Router: A router performs all the functions of a bridge. In addition, it can connect heterogeneous local area networks and also determine networks traffic over the fastest channel between two nodes in different sub-networks (e.g. It determines network availability by examining traffic patterns within a network and also between different networks.
Gateway: Gateways are the most complex of the three networks connection devices. Their primary function is to perform protocol conversion, so that different types of

communication architectures can communicate with one another. The gateway identifies maps the functions performed in an application on one computer with the similar functions performed by a different application on another computer.

3.7.4 Processing Controls

The processing subsystem is responsible for computing, sorting, classifying, and summarizing data. Its major components are

1. The Central Processor where programs are executed,
2. The real or virtual memory in which program instructions and data are stored,
3. The operating system that manages system resources, and
4. 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 program from memory and determines their type; (b) an Arithmetic and Logical Unit, which performs operations; and (c) Registers, which 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 as follows.

- **Error Detection and Correction:** Processors might malfunction occasionally due to design errors, manufacturing defects, damage, and electromagnetic interference. Various types of error detection and correction strategies must be used.
- **Multiple Execution States:** It is important to determine the number and nature of execution executed by the processor. This will help auditors to determine which processor will be able to carry out unauthorized activities, such as gaining access to sensitive data.
- **Timing Controls:** An operating system might get stuck in many loops. In such a situation and in the absence of any control, the program will retain use of processor and prevent other programs from undertaken their work.
- **Component Replication** In some cases, processor failure can result in significant losses. Out dated processors should be used to detect and correct errors. If processor failure is permanent in multicomputer or multiprocessor, the system might reconfigure itself to isolate the failed processor.

ii. **Real Memory Controls:** This comprises the fixed amount of primary storage in which data must reside which must be executed by central processor. Real memory controls seek to detect and correct errors that occur in memory cells and also

protect areas of memory assigned to a program from illegal access by another program.

iii. **Virtual Memory Controls:** Virtual Memory exist when the addressed storage space is large than 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.