PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

Chap 1 :

COBIT 5 : 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.

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.

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 model 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 define its own process set, taking into account its specific situation.

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

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.

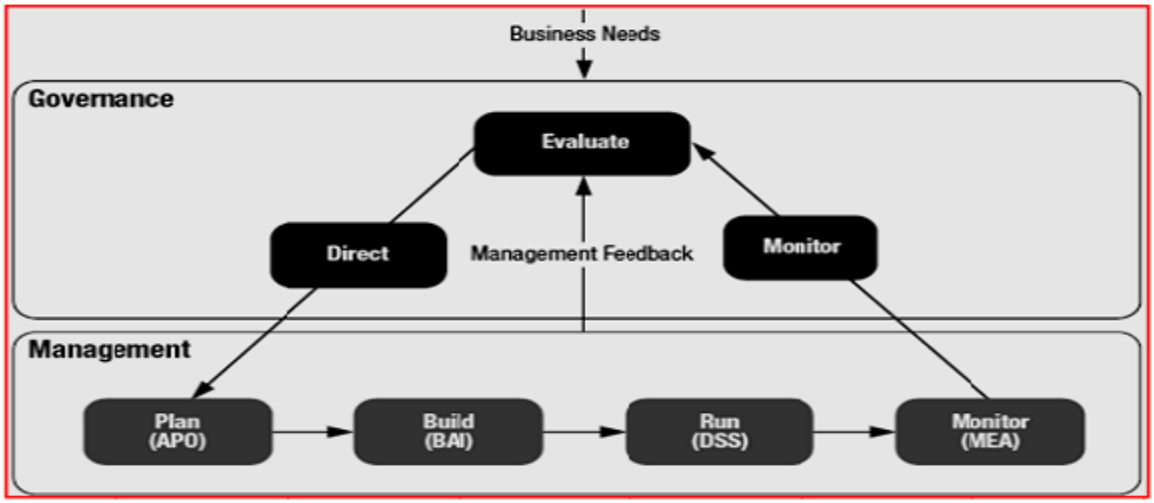


Fig. 1.10.3: Key Areas of Governance and Management*

Governance: It ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most of the enterprises, overall governance is the responsibility of the Board of Directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

Management: It contains four domains, in line with the responsibility areas of Plan, Build, Run and Monitor (PBRM). providing the end-to-end coverage of IT in alignment with the direction set by the governance body to achieve the enterprise objectives. In most of the enterprises, management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO).

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)

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

Chap 2 :

(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, labor & capital (i.e. three most important production factors). 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.

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.

(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 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

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

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 FinnOne 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

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

Chap 3 :

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 often results in the errors. Therefore, it is difficult to find competent and trustworthy information systems 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 trail 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, transactions etc. are placed properly, it will not be a problem for auditor.
- **Physical Control over Assets and Records:** In manual systems, protection from unauthorised 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 result 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 enable employees to be closer 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.

APPLICATION CONTROL :

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 subsystem are as follows:
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: 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: • Increases 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 associated 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. Furher, 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 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 area within a few kilometers). 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 include 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
They are implemented using 3 tyoes of topologies: (1) Tree topology, (2) Ring topology, and (3) Star topology.

(f) Channel Access Controls: Two different nodes in a network can compete to use a communication channel. Whenever the possiblility of dispute 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:** 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 compete 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 network 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 network 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 network 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.

3.8.4 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 programs 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 undertaking 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 exists when the addressed storage space is larger 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.

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

Chap 6 :

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.

PROF .JIGNESH CHHEDA
Chheda.jignesh@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.

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.

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

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 beforeimages 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

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

chap 7 :

ISO 27001

ISO/IEC 27001 (International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC)) defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large. It is a standard written by the world's best experts in the field of information security and aims to provide a methodology for the implementation of information security in an organization. ISO/IEC 27001 formally specifies an **Information Security Management System (ISMS)**, a suite of activities concerning the management of information security risks.

The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts.

Given the importance of ISO 27001, many legislatures have taken this standard as a basis for drawing up different regulations in the field of personal data protection, protection of confidential information, protection of information systems, management of operational risks in financial institutions, etc.

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

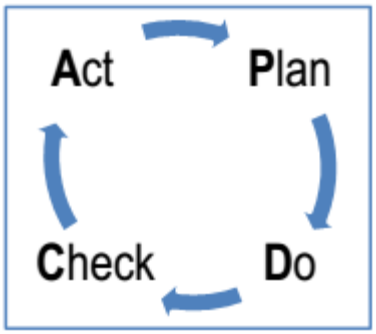
ISO/IEC 27001 is derived from The British Standard BS 7799 Part 2, published in 1999. BS 7799 Part 2 was revised by BSI in 2002, explicitly incorporating Deming's PDCA process concept, and was adopted by ISO/IEC as ISO/IEC 27001 in 2005. It was extensively revised in 2013, bringing it into line with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

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

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.

(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.

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

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

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

Annex A: List of controls an 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.

Benefits of ISO 27001

The key benefits of ISO 27001 are given as follows:

- It can act as the extension of the current quality system to include security.
- It provides an opportunity to identify and manage risks to key information and systems assets.
- Provides confidence and assurance to trading partners and clients; acts as a marketing tool.
- Allows an independent review and assurance to you on information security practices.

PROF .JIGNESH CHHEDA
Chheda.jignesh@gmail.com

A company may adopt ISO 27001 for the following reasons:

- It is suitable for protecting critical and sensitive information.
- It provides a holistic, risk-based approach to secure information and compliance.
- Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.
- Demonstrates security status according to internationally accepted criteria.
- Creates a market differentiation due to prestige, image and external goodwill.
- If a company is certified once, it is accepted globally.