Chapter-5 Amendments:

There are a few amendments in this chapter but those are more related to elementary addition to content which was already there.

Please find below the new additions in this chapter. Please note that all the topics are as it is there in the earlier published chapter-5. Please study the below revisions in addition to whatever is provided in the chapter-5. Please note that Risk Assessment Forms given at the end of chapter-5 in my ISCA book are deleted now.

1.0 Introduction:

In the current networked environment the threats and attacks to information system have increased. Therefore, the risk assessment has become more important to organization. Additionally, industrial bodies and government also recommending and pressurizing for use of risk assessment and security techniques.

2.0 Risk Related Terms:

Asset: Asset can be defined as something valuable to organization like information, employees, server etc. Asset can be defined as:

- Has value for organization
- Not easily replaceable without cost, skill, time and resources etc
- Form a part of organization's identity
- Information asset can normally be classified as: top secret, highly confidential, proprietary, internal and public

Vulnerability: Vulnerability can be referred as weakness in the software and system which can be exploited by the attackers. The vulnerability normally originates from flaw in software design, defects in implementation or problems in operation. Normally, vulnerability is defined as opening door for attackers. It has the following implications:

- Allows an attacker to unauthorized access and copy data
- Allows an attackers to execute and insert malicious programs
- Allows and attackers to conduct attack like denial of service attack

Threat: A threat is an action, event or condition which causes compromise with system integrity and quality and causes harm to organization. Threats and assets are closely related because a threat cannot exist without a target asset.

Attack: Attack is an attempt to gain unauthorized access to system. It is an intentional malicious act for causing harm to system.

Risk: Risk can be defined as potential harm, if a particular threat exploits a particular vulnerability and causes harm to system. Risk analysis is determining the magnitude of harm.

Countermeasure: This is an action, device, procedure or technique which can reduce the vulnerability. This is technically control which helps to protect system e.g. antivirus, login-id password etc.

3.0 Threats to Computerized environment:

Errors and Omissions: This is an important threat to data and integrity. These errors are normally caused by data entry operators

Malicious code: Malicious code refers to virus and destructive programs which can cause harm to system e.g. Trozan Horse, Worm and Logic bomb etc.

4.0 Threats to Cyber Crime:

Denial of Service Attack: In this attacker by using some technique known as IP Spoofing block the organization's site or system from providing services to authorized users. The organization's system is attacked in such a manner that when an authorized user wants to access the system or site he is given a message like server is busy or page not available etc. The organization's system or site remains unavailable for hours or days from providing services to authorized users.

Chapter -8 Amendments

In this chapter, the following topics are completely revised in the latest Jan, 2013 study:

(1) ISO 27001
(2) CMM
(3) COBIT
(4) CoCo
(5) ITIL

The following topic has been introduced as new topic

(1) SA 402. This students will primarily read this in the Audit paper

The following topics are deleted from this chapter:

(1) ValIT and RiskIT
(2) COSO
(3) SAS 70

Please study the above revised topics from the following amended content.

1.0 ISO 27001 – Information Security Management Standard:

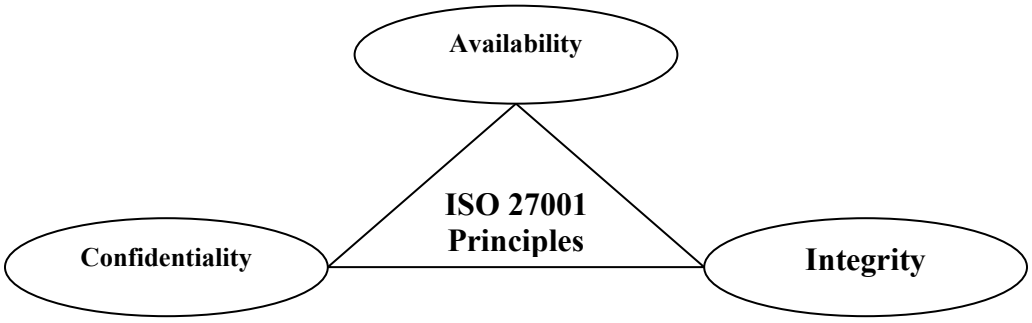
The essence of ISO 27001 is that a sound Information Security Management System ***(ISMS)*** should be established within the organization. The purpose of this is to ensure that an organization's information is secured and properly managed.

ISO 27001 states that Information is an asset which likes other important business assets has value to an organization. Therefore, information needs to be suitably protected using security measures or controls

As per ISO 27001 Information security should be based on the following key principles.
a) Confidentiality: ensuring that information can only be accessed by those who have proper authorization;

b) Integrity: safeguarding the accuracy and completeness of information;

c) Availability: ensuring that authorized users have access to information and associated assets whenever required.

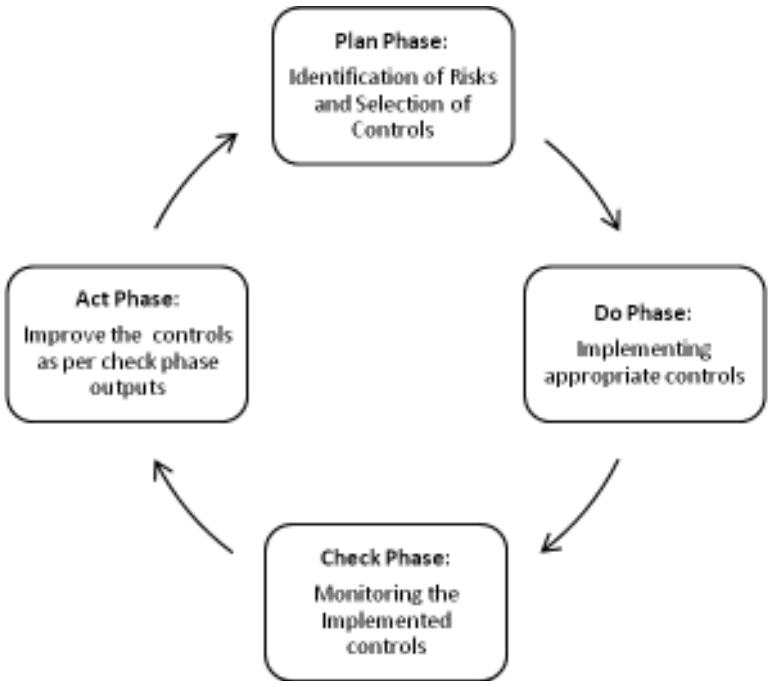


ISO 27100 is considered as the most influential, globally recognized standard for information security This is the also considered international best practice for information security management. ISO 27001 is also known as ISMS (Information Security Management System) provides a systematic approach for managing confidential and sensitive information. ISO 27001 is to the information security just like ISO9001 is for the quality.

Quality Standard Information Security

ISO 27001 defines how to organize information security in any organization. It is a standard written by best security experts in the fields of information security and it provides methodology for implementing information security in the organization. It also enables to get certified for information security like organizations get certified for quality.

Four Phases of Information Security Management System (ISMS):
ISO 27001 or ISMS describes four phases for planning, implementing and managing information security.



Phase-1 - The plan Phase:
This phase, as its name suggests, provides series of steps for planning information security. It helps to set objectives for information security, indentify and assess risks and select the appropriate controls. This phase consists of the following key steps:

- Determining scope of ISMS and writing an ISMS policy
- Identifying methodology for risk assessment
- Identification of assets, vulnerabilities and threats

- Evaluating risks and risks treatment options
- Selection of controls
- Obtaining management approval for controls and residual risks

Phase-2: The Do Phase:
This phase includes the following key activities:

- Documenting the risk treatment plan i.e. describes who, how, when and with what budget the controls should be implemented
- Implementing the risks treatment plan
- Implementing applicable security controls
- Determining how to measure the effectiveness of controls
- Carrying out awareness programs and training of employees
- Managing ISMS resources and implementation of procedures for detecting and managing security incidents

Phase-3: The Check Phase:
This phase consists of the following activities:

- Implementation of procedures for monitoring and reviewing of controls for establishing any violation, incorrect data processing
- Finding whether the security activities are carried out as expected.
- Regular reviews of the effectiveness of the ISMS
- Measuring effectiveness of controls
- Reviewing risks assessment at regular intervals
- Internal audits at planned intervals
- Identify opportunities for improvement
- Updating security plans taking into account of monitoring and reviewing activities
- Keeping records of activities and incidents that may affect the effectiveness of the ISMS

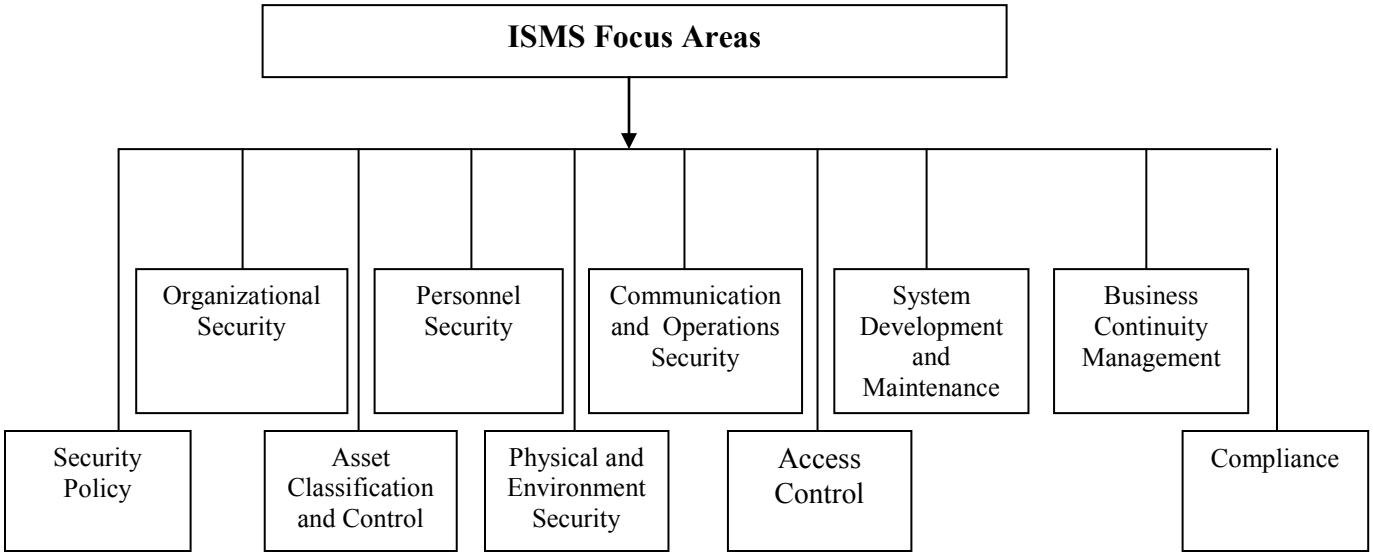
Phase-4: The Act Phase:

- Implementation of identified improvements in the check phase
- Taking corrective and preventive actions applying security experiences
- Communicating activities and improvements to all stakeholders
- Ensuring that improvements achieve desired objectives

Other Standard Related to Information Security:
In addition to ISO-27001 (formerly known as BS7799-2), ISO 27002 (formerly known as ISO 17799) is an auxiliary standard and provides more details for implementing ISO 27001 controls. Other standards which can be useful for security are ISO 27005 which describes risk assessment procedures in more details and BS 25999-2 which provides a detailed description of Business Continuity Plan.

FOCUS area of ISMS:

There are ten focus areas of ISMS,



SECURITY POLICY:

This focus area describes that organization should form a security policy like other business policies to have a better information security management. A security policy primarily covers:

- The organization's requirements for information security
- The scope of the information security, including business functions, areas and sites to be covered
- The general philosophy towards information security

To have an effective policy, it should be clearly supported by senior management.

ORGANISATIONAL SECURITY:

This focus area describes that there should be management framework or organizational structure to support information security. The organizational security specifications describe:

- How the organization should manage their information security
- The responsibilities of each relevant person, committee or forum. Also, includes responsibilities for creating and revising procedures and policies for information security.

An organizational security structure also describes:

- Staff who can be contacted when help or advice is needed
- Staff who should be reported for security problems and system difficulties

ASSET CLASSIFICATION & CONTROL:

This focus area describes that different information assets should be classified as per their value and controls should be applied accordingly.

In general, organizations maintain different types of physical assets e.g. computers, printers, machinery and vehicles etc. Information is also recognized as a vital asset for every organization. The value of specific information will depend on factors such as:

- How much it cost to obtain the information
- The extent of damage done to the organization if it was disclosed to the public or a competitor

The specifications for this focus area describes that an Information Asset Register (IAR) should be created, detailing every information asset within the organization. For example:

- Databases
- Personnel records
- Software Designs
- Test Results
- Developed Software / Programs
- Contracts
- Software licenses

The Information Asset Register (IAR) should also describe:

- Who is responsible for each information asset
- Any special requirements for confidentiality, integrity or availability of information

The value of each asset can be determined to ensure appropriate security is in place.

PERSONNEL SECURITY:

This focus area describes that it is very important to control human errors and frauds which are key reasons of breach of information security. This security describes the job definitions to reduce the risk of human error and ensure that staff understands what their rights and responsibilities are related to information security:

Appropriate personnel security ensures that:

- Employment contracts and staff handbooks have agreed and contains clear wording on job descriptions
- Ancillary workers, temporary staff, contractors and third parties are covered in job definitions
- Anyone else with legitimate access to business information or systems is covered in handbook

Staff training is an important feature of personnel security to ensure the Information Security Management System (ISMS) continues to be effective.

PHYSICAL AND ENVIRONMENTAL SECURITY:

This focus area deals with physical access control of information and information systems. This security ensures that there are proper controls for systems, records and staff, etc., essential for maintaining confidentiality, integrity and availability of information.

The following aspects should be considered in this security:

- Protection of information and information systems from unauthorised people.
- Physical access should be restricted to authorised personnel only.

COMMUNICATIONS AND OPERATIONS MANAGEMENT:

This is the largest section of ISO 27001. This section describes that the day-to-day operation of IT systems is fundamental to most organizations, particularly for organizations using online systems such as banks and telecom, etc. The specifications on keeping IT and communications systems security are covered in this section. Many of the specifications covered in this section apply to every IT system, irrespective of size, purpose, internal or external operation. And this section includes detailed specifications on:

- Networks
- Handling computer media
- Electronic commerce
- E-mail
- Publicly available systems (such as websites)

Moreover, this is a frequently changing area of security. New viruses and hacking opportunities are the most publicized issues. However, many incidents are caused by poor system design and management rather than malicious actions. Good security practice in communications and operations management ensures efficient and effective business systems.

ACCESS CONTROL:

This focus area describes that logical access controls and review of these controls are important to ensure that information and applications are accessed by authorized users only. Access control is about managing access of users to:

- Information
- Computer applications
- Operating system facilities

Effective access control ensures that only authorized users are given access of resources and per their access rights. Confidentiality of information is best achieved by ensuring that people only have access to the information they actually need.

If access rules are too detailed, managing them will be very difficult. If they are too general, people will have access to information or applications to which are not authorized to access. A balance must be struck depending on:

- Needs of the business
- Security features provided by the systems
- Trust in staff

Normally following features helps in providing good access control

- Implementation of strong password policy
- Appropriate management of access rights for read, update, insert or delete of information

- Analysis of what users require to access for their job
- Analysis of the security features that each system can provide

SYSTEM DEVELOPMENT AND MAINTENANCE:

Designing a new system with security in mind provide more effective security for a system than if we attempt to impose security after developing the system.

ISO 27001 specifies that following should be considered while developing and maintaining a system:

- Specify security requirements during system requirement and analysis
- Specify required application security
- Specify use of data encryption or cryptography
- Specify the security of system files

BUSINESS CONTINUITY MANAGEMENT:

Each organisation's business relies on its own staff, systems and, to some extent, other organisations. Anything from a burst water pipe to a terrorist attack can have a major effect on organisation. As such, there must be a process for managing business continuity plans.

Business continuity management considers the risks within an organisation and ensures that core processes keep running during adverse events. A review procedure to ensure that the plans are workable, and are sufficient to cover the most likely occurrences, is also necessary.

COMPLIANCE:

Every organisation is required to comply with its country law. Within the scope of the Information Security Management System (ISMS), each organization should list the main laws that affect its activities.

These may include:

- Health and Safety legislation
- The Data Protection Act
- The Information Technology Act
- The Designs, Copyrights and Patents Act
- The Human Rights Act

Compliance with these is a legal requirement, and implementing ISMS is a good way of ensuring that business does comply with required compliance.

CERTIFICATION

Certification to BS ISO 27001 is a formal acknowledgement that your Information Security Management System (ISMS) reflects your organisation’s information security needs.

2.0 CMM – Capability Maturity Model:

This model provides guidelines for organization involved in the software developments to develop high performance software.

Software engineering Institute (SEI) in cooperation with Mitre Cooperation developed the CMM for software. CMM is model of process maturity for software development which is evolutionary model of the progress of company's abilities to develop software. The CMM presents sets of recommended practices in number of key process areas that have been shown to enhance software process capabilities. The CMM is based on knowledge acquired from software process assessments and extensive feedback from both industry and government.

CMM guidelines are used by software organization such as Infosys and Wipro, etc to gain control on their processes for developing software. And it also helps such organizations to evolve a culture of software engineering and management excellence.

CMM helps software organization to improve organization-wide software development processes to achieve continuous and lasting gains in software development capability.

Fundmanetals concepts of Capability Maturity Model

Software process consist of set of activities, methods and procedures that developers use to develop and maintain software and associated products, such as – designs, code, test procedures and documents, etc. As organizations become more mature, the software processes become more defined and consistent.

There are numerous fundamental concepts related to capability model, such as;

Capability:
Describe the range of expected results that can be achieved by following a software process. The software process capability of an organization provides means of predicting the most likely outcomes to be expected from the next software project the organization undertakes.

Performance:
Represents the actual results achieved through follow-up of a software process. Thus, software process performance focuses on the results achieved, while software process capability focuses on results expected.

Maturity:
Software process maturity is thus defined, managed, measured and controlled process in the organization for software development. Maturity implies potential for growth in capability and also indicates richness of organization software's process. Software process maturity also help organization to under-take more projects and also help to predicts timely delivery and the quality output of under-taken projects.

Five Levels of Software Process Maturity:

Many companies had been contemplating significant overrun in schedule and budget. The development and application of CMM helps to solve this problem. The key concept of this standard is organizational maturity. A mature organization clearly defines procedures for software development and project management. These procedures are adjusted and perfected as required.

As per SEI: The five levels for the CMM can be defined as:

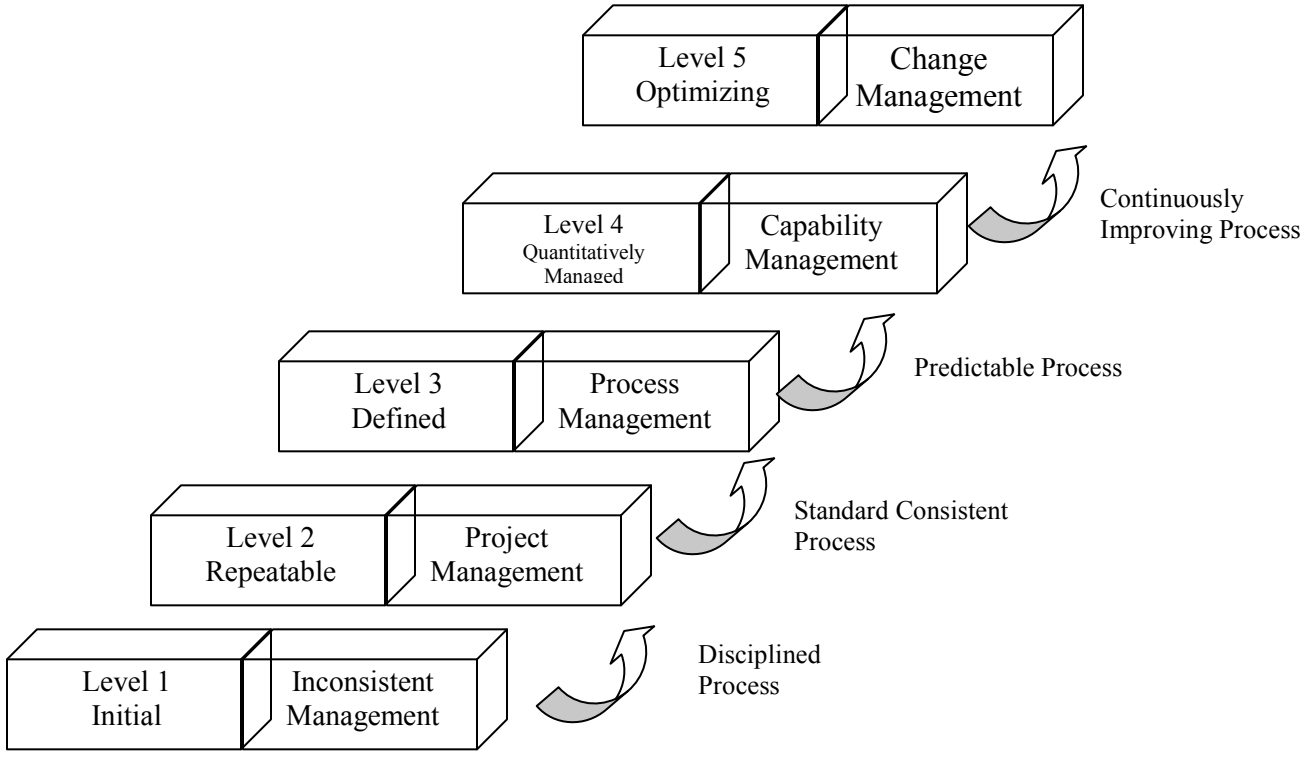
(1) Initial: at this level either the process is new or process is not documented

(2) Repeatable: The process is at least documented sufficiently such that repeating the same stapes may be attempted efficiently

(3) Defined: The process is defined and confirmed as standard business process with clear instructions on how to use the process.

(4) Managed: At this level, the process is quantitatively managed in accordance of agreed upon metrics including time, cost and resources use

(5) Optimizing: at this level, management includes deliberate process improvement and optimization factors



During the evolution through the five maturity levels, development practices are transformed from an ad-hoc, undisciplined state into disciplined processes capable of predictable results. At its core, the CMM is a unique model of organizational development and change. As organization progresses from one level to the next, its culture is transformed through the evolutionary improvement of its development processes.

Behavior Characterization of Maturity Levels:

Maturity level 2 through 5 is primarily described as levels used by organization to improve the software processes. The description below provides behaviors characterization of processes at various CMM levels.

(1) **Initial Level:** The key characteristic of processes at this level is that the processes are undocumented. The processes are performed in adhoc, uncontrolled and reactive manner by users. This level provides unstable and chaotic environment for the processes.

- At this base level, application development practices and results are inconsistent.
- Development processes rarely are defined, and sound practices often are sacrificed to meet unreasonable schedules.
- Although developers are capable of performing their assignments but they do so through individualized methods that shows consistency across the organization.

Essentially, the Level 1 organization lacks the capability to meet commitments consistently.

(2) **The Repeatable Level:** The key characteristic of processes at this level is that the processes are repeatable and can provide consistent results. The process discipline is not very high but it helps to conduct processes with discipline during time of stress.

- Level 2 focuses on developing the capabilities of project managers to plan achievable commitments
- Organizations establishes controls to track progress of projects which help to establish stable environment
- Although projects may use different methods or practices, the environment must be stabilized to support their performance.

Organizations with Level 2 capabilities deliver their applications on schedule without having to survive constant overtime and on particular individuals.

(3) **The Defined Level:** The key characteristic of processes at this level is that the processes are well defined and documented with set of standards. The processes provide consistent performance across organization and everyone uses same set of standards for processes.

- After projects can repeat successful practices, organizations identify best practices from different projects. Subsequently, these procedures are integrated into a common Application Development process and deployed across the organization.
- Hence, a strong organizational culture emerges at Level 3 based on a common process that covers all the important elements of Application Development.

Organizations with Level 3 have defined processes or common processes for application developments, which helps them to achieve targets for cost, functionality and scheduling.

(4) **The Managed Level:** At this level process characteristics are further improved by putting together controls which helps to provide the desired results even in adverse situation. The management can assess the adjustment required in the processes to provide the high quality of results. The process capability is actually established from this level.

- Having established defined or common Application Development processes, an organization then can develop statistical capability that can quantify the expected results from performing defined procedures.
- These quantifications provide baselines of development processes and help to measure the variation and their causes in the actual performance.
- By managing the performance of its development processes statistically, an organization can predict the project outcomes much earlier in the course of a project.

Quantitative management increases the predictability of results for project management.

(5) The Optimizing Level: At this level the management acquired the capabilities to further improve the processes by adopting new innovative methods and technology changes

- Despite the achievement of predictable results, targeted business objectives may not be achieved.
- At Level 5 an organization continuously evaluates the capability of its processes to pinpoint areas requiring the greatest improvement.
- Continuous improvements can be developed by deploying the results of lessons learned, or they can be produced by evaluating new development methods, processes or technologies for potential adoption.

Ultimately, a Level 5 organization establishes an infrastructure for supporting continuous change management as a fundamental, integral component of its overall development process.

As a software development organization proceeds from one maturity level to the next, the range of benefits from its improvement activities and processes increase substantially. Since improvements at each maturity level solve different sets of problems, different benefits emerge at each level.

3.0 COBIT – The IT Governance Model:

COBIT is known **C**ontrol **OB**jectives for **I**nformation and related **T**echnology. COBIT is known as IT governance model because it specifies the standards for information security and IT controls.
In General, COBIT is defined as below:

- COBIT (Control Objectives for Information and Related Technology) is globally accepted as the most comprehensive work for IT governance and risk management
- COBIT provides good practices for the management of IT system in a manageable and logical structure.
- COBIT meets the multiple needs of enterprise management by bridging the gaps between business risks, technical issues, control needs and performance measurement requirements.

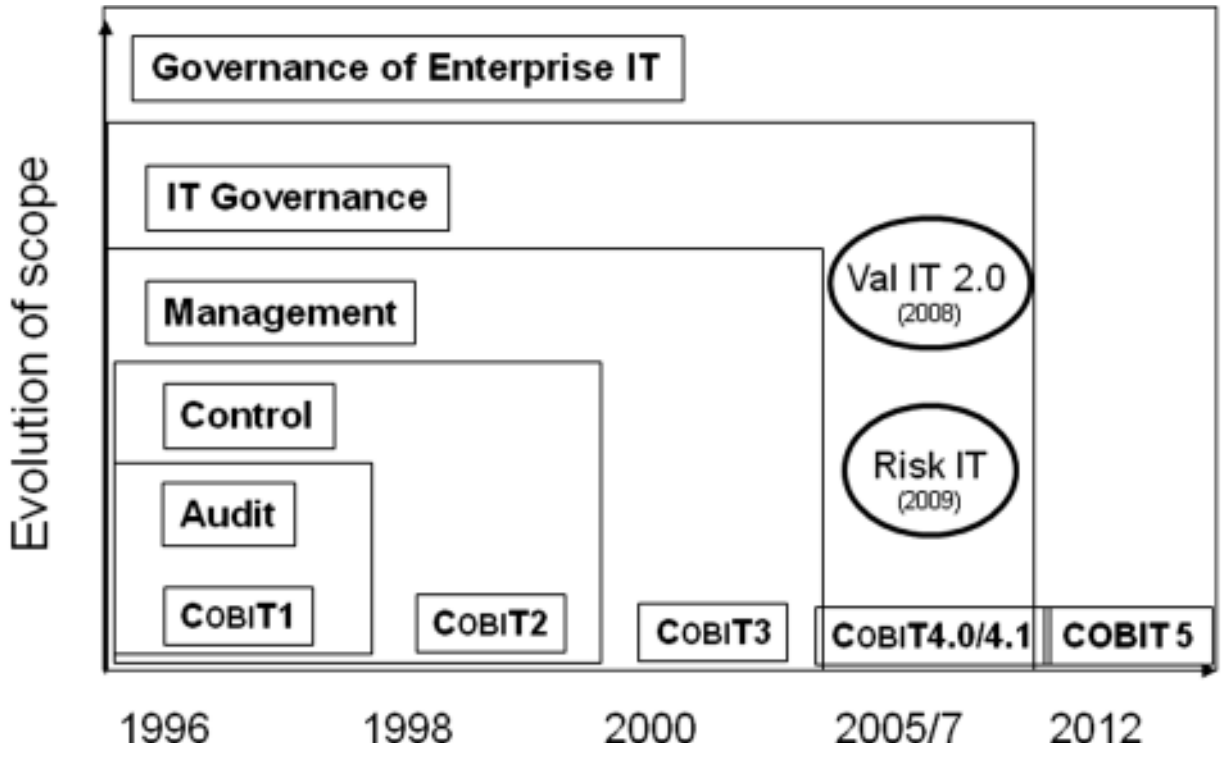
- The COBIT mission is to research, develop and promote an up-to-date international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.

COBIT has been revised many times since its inception. It has the following major releases:

- In 1996 first edition of COBIT was released
- In 1998, the second edition added "Management Guidelines"
- In 2000, the third edition was released and in 2003 online version become available
- In 2005, the fourth edition was released and in May 2007 current COBIT 4.1 version was released
- In 2012, the fifth version known as COBIT 5 was released

COBIT 5:

COBIT 5 is the only business framework for the governance and management of enterprise IT. It helps to integrate the business practices with IT. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, and analytical tools and models which to get maximum value from information systems. COBIT 5 builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO).



Evolution of COBIT Model

Need for COBIT 5

COBIT 5 helps enterprises create optimal value from their information and technology. Enterprises depend upon good reliable repeatable data on which they can base good business decisions. COBIT 5 provides the tools necessary to understand, utilize, implement and direct important IT-related activities to make more informed decisions. COBIT 5 is intended for enterprises of all sizes including non-profit and public sector and it is designed to deliver business benefits to business including:

- Increased value creation for use of IT
- User satisfaction with IT engagement and services
- Reduced IT related risks and compliance with laws and regulations and contractual requirements
- The development of more business focused IT solutions and services
- Increased Enterprise vide involvement in IT-related activities

Benefits of COBIT 5

COBIT 5 helps all size of organizations for IT governance. It provides the following benefits.

- Maintain high-quality information to support business decisions
- Achieve strategic goals and realize business benefits through the effective and innovative use of IT
- Achieve operational excellence through reliable, efficient application of technology
- Maintain IT-related risk at an acceptable level
- Optimize the cost of IT services and technology
- Support compliance with relevant laws, regulations, contractual agreements and policies

Integrating COBIT5 with other Framework:

COBIT 5 is very comprehensive framework. COBIT 5 provides a basis for integrating effectively with other frameworks such as ITIL and ISO 27000 etc. It is also very well aligned with other ISO standards. Thus COBIT-5 may act as single overall framework which will provide both non-technical and technical source of guidance for meeting business objectives. The COBIT 5 framework and its enablers can be aligned with:

- Enterprise policies, strategies, governance, business plans and audit approaches
- Enterprise Risk Management Framework
- Existing enterprise structure and processes.

COBIT 5 principles:

COBIT 5 brings together the five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of stakeholders.

As its name suggests the COBIT 5 has the 5 key principles:

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management

(1) Meeting Stakeholder Needs:

We know that enterprises exist to create value for their stakeholders by maintaining a balance between the benefits and risks by optimum use of resources. COBIT 5 provide all the required processes for creating value for business by using IT. COBIT 5 describes that every organization has different objectives and goals and it allows organizations to customize their goals and link those goals to IT- related goals, and apply those to organization processes for creating value for business.

(2) Covering the Enterprise End-to-end:

COBIT 5 helps to integrate organization governance with IT-Governance. It covers all functions and processes within the organization. **COBIT 5 does not focus only on the 'IT function'**, but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.

(3) Applying a Single Integrated Framework:

There are many IT-related standards and each provides guidelines on set of IT related activities. COBIT 5 is a single and integrated framework and it aligns with the other standards and frameworks used by enterprises like COSO and ISO 27001. This allows the enterprise to use COBIT 5 as an overall governance and management framework integrator.

(4) Enabling a Holistic Approach:

COBIT describes that efficient and effective governance and management of enterprise IT require a holistic approach taking into account several interacting components. COBIT 5 defines set of enablers to support implementation of comprehensive IT governance. These enablers are categorized as 7 enablers and help to achieve objectives of enterprise.

(5) Separating Governance from Management:

The COBIT 5 framework makes a clear distinction between governance and management.
These two disciplines:

a. Encompass different types of activities
b. Require different organisational structures
c. Serve different purposes

Governance—In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson. It ensures that stakeholders needs, conditions and options are **evaluated** in order to determine and achieve a balanced and agreed-on enterprise objectives

Management—In most enterprises, management is the responsibility of the executive management under the leadership of the CEO. **Management plans, builds, runs** and **monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives

COBIT advocates that organization implement governance and management processes such that the key areas are covered.

Enablers of COBIT 5

The COBIT 5 framework describes seven categories of enablers:

- **Principles, policies and frameworks:** These are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures:** are the key decision-making entities in an enterprise.
- **Culture, ethics and behavior** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
- **Information** is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, infrastructure and applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, skills and competencies** are required for successful completion of all activities, and for making correct decisions and taking corrective actions.

COBIT 5 Process Reference Model:

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

4.0 CoCo:

The Criteria for Controls (CoCo), was published in 1995 by The Canadian Institute of Chartered Accountants (CICA). This model is considered an extension of COSO. CoCo can be said to be a concise superset of COSO.

What is COSO?
The Committee of Sponsoring Organizations–COSO: This is an internal control integrated framework. The major accounting and audit professional organizations in the US issued COSO in 1992.

As per COSO, internal control is:

- a process,
- effected by an entity's board of directors, management, and other personnel,
- designed to provide reasonable assurance regarding the achievement of objectives

As per CoCo, internal control is:

- those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the objectives

CoCo does not cover any aspect of information assurance. It is concerned with controls in general. It uses the three categories of objectives for controls:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

CoCo describes the four important interrelated fundamental of controls:

- Purpose
- Capability
- Commitment
- Monitoring and learning

Additionally, CoCo describes the four important concepts about control:

- Control is effected by people including board of directors, management and staff
- People responsible for achieving organization objectives should also be responsible for achieving effectiveness of controls
- Organizations constantly adapt and improve
- Control can be expected to provide reasonable assurance.

.

5.0 ITIL (IT Infrastructure Library):

The Information Technology Infrastructure Library (ITIL) is a public framework that describes best practices in IT Service Management (ITSM). It key focus is to align IT services with business needs. Additionally, it focuses on the continual measurement and improvement of the quality of IT services delivered, from both a business and a customer perspective. The reason behind the development of ITIL is the recognition that organisations are becoming increasingly dependent on IT in order to achieve their business objectives and meet their business needs. This leads to an increased requirement for high quality IT services.

ITIL describes procedures, tasks and checklist for establishing a minimum level of competency and quality for IT services.

History of ITIL

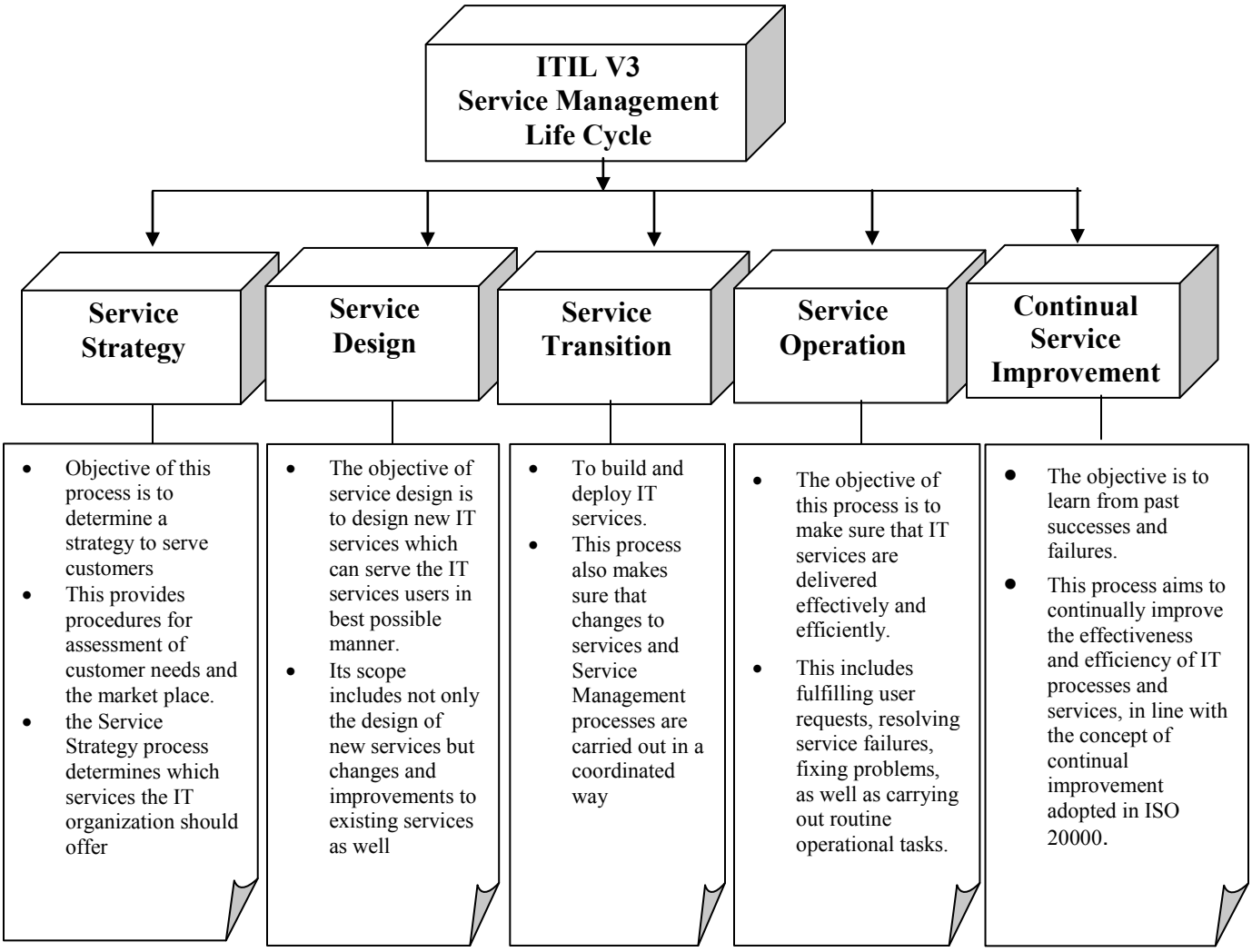
UK Govt. originally created the ITIL. However, it has been adopted across the world as best practices for providing IT related services. We know that IT services have become closely integrated with business and ITIL assists in integrating business and IT services in best possible manner to provide maximum benefits of IT services to business. The key objective of any service management is transform resources into valuable services and ITIL helps to achieve this objective.

The ITIL has been improved over the years and since its first version (ITIL V1) it contains the set of books on IT service management. The initial version of ITIL i.e. ITIL V1 consisted of a set of 31 associated books covering all aspects of IT service provision. This initial version was then revised and replaced by eight, more closely connected and consistent books (ITIL V2) consolidated within an

overall framework. This second version became universally accepted and used in many countries by thousands of organizations as the basis for effective IT service provision. In 2007, ITIL V2 was superseded by an enhanced and consolidated third version of ITIL V3, consisting of five core books covering the service management and lifecycle.

The ITIL V3 Library consists of five books

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement



ITIL V3 Processes

(1) Service Strategy:

Objectives:

- The key objective of this process is to determine a strategy to serve customers
- This provides procedures for assessment of customer needs and the market place.
- the Service Strategy process determines which services the IT organization should offer

The Service Strategy publication or book is the core of the ITIL V3 lifecycle. It sets out guidance to IT service providers and helps them to build a clear service strategy. It describes that the service strategy adopted must provide sufficient value to the customers and to the service provider – it must fulfill the service provider's strategic purpose. Irrespective of the context in which the service provider operates, its service strategy must also be based upon a clear recognition of the existence of competition. It describes that each competitor has choices and it provides procedures, how a service provider will differentiate itself from the competition.

(2) Service Design:

Objectives:

- Design new IT services which can serve the IT services users in best possible manner.
- Its scope includes not only the design of new services but changes and improvements to existing services as well

Service Design is an important stage within the overall service lifecycle. It provides guidelines for design of appropriate and innovative IT services, including: structure, logics, rules and documentation for services to meet current and future business requirements.

(3) Service Transition:

Objectives:

- To build and deploy IT services.
- This process also makes sure that changes to services and Service Management processes are carried out in a coordinated way

The role of Service Transition is to deliver services that are required by the business into operational use. Service Transition stage provides procedures and guidelines to convert design into operation. It also provides procedures to implement any changes required since design in order to deliver the required services. Service Transition focuses on implementing all aspects of the service, not just the software and hardware; it helps to implement rules and procedures to use the services in most efficient and reliable manner.

(4) Service Operation:

Objectives:

- The objective of this process is to make sure that IT services are delivered effectively and efficiently.
- This includes fulfilling user requests, resolving service failures, fixing problems, as well as carrying out routine operational tasks.

It provides procedures and guidelines for managing efficient operation of services to ensure that agreed levels of services are delivered to users and customers. It also helps to manage the applications, technology and infrastructure that support delivery of the services. It describes that it is only during this stage of the lifecycle that services actually deliver value to the business, and it is the responsibility of Service Operation staff to ensure that this value is delivered.

(5) Continual Service Management:
Objectives:

- Learn from past successes and failures.
- This process aims to continually improve the effectiveness and efficiency of IT processes and services, in line with the concept of continual improvement adopted in ISO 20000.

Continual Service Improvement (CSI) combines principles, practices and methods from quality management, Change Management and capability improvement. This helps to improve each stage in the service lifecycle and also helps to improve the current services, processes, and related activities and technology. CSI stage describes that maintaining value for customers through the continual evaluation and is very important to improve the quality of services and the overall maturity of the ITSM service lifecycle and underlying processes. For many organizations, CSI becomes a project when something has failed and severely impacted the business.

6.0 SA 402

SA 402 is a revised version of the earlier Audit and Assurance Standard (AAS) 24 "Audit consideration Relating to Entity Using Service Organization" issued by the ICAI in 2002. The revised standard deals with user auditor's responsibility to obtain sufficient and appropriate audit evidence when a user entity uses the services of one or more service organizations.
SA 402 deals with the following aspects for audit of service organization:

- Obtaining an understanding of services provided by service organization
- Obtaining understanding of internal controls
- Responding to assessed risks of material misstatement
- Type-1 and Type -II Report
- Fraud, non-compliance with laws and regulations
- Uncorrected misstatements in relation to activities at the service organization
- Reporting by the user auditor

Please read this from the audit study for more detail on this