AMENDMENTS BY ICAI

MADE BY

CA AKHIL MITTAL

B.com (H)-SRCC, ACA

Chapter 5

RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

A. *INTRODUCTION:*

In the current interconnected world, there is an urge for the use of a full proof information system. But this information is open to threats due to easy accessibility by almost every individual.

Any information which is open for easy accessibility is vulnerable to threats. So in past few years **risk assessment** has been important for every organisation.

B. *RELATED TERMS:*

Various terminologies related to risk assessment→

ASSET:

Asset can be defined as **SOMETHING OF VALUE** to the organisation.

E.g.: **Information in electronic or physical form**

Software system, employees

Following are the characteristic of assets:

1. **They are recognised to be value to the organisation.**
2. **They are not replaceable without** cost, skill, time or resources.
3. **They form part of the organisation without which organisation may be threatened.**
4. **Their data classification is** proprietary, highly confidential or even top secret.

VULNERABILITY:

It can be referred as the weakness of the software which is exploited by the attackers. It is originated from the flaws in software design, implementation defects, or other problems in its operation.

If I want to sum the **"nature of vulnerability"** then we can do it by:

ALLOWS:

-- **An attacker to execute commands as another user.**
-- **An attacker to access data which is rather restricted to be accessed.**
-- **An attacker to pose as another entity.**
-- **An attacker to conduct denial of services.**

THREAT:

- Any entity, circumstances or event with the potential,
- To harm the **software systems or component**
- Through **its unauthorised access, destruction, modification**
- Is called a ***THREAT.***

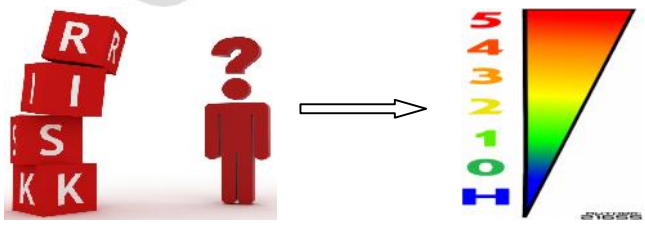
I am hereby enumerating the characteristics of the threat:

- It is action/event/condition where there is a compromise in the system
- Negative impact on the quality of the system.
- Threat has the capability to attack on the system with the intent to harm it.

RISK :

- RISK = **Potential harm caused if threat** *exploits* **a particular vulnerability to cause damage to an asset.**

- RISK ANALYSIS = **It refers to process of** identifying **the security risk & determining their** magnitude **and** impact **on the organisation.**



Identifying RISK **MAGNITUDE & IMPACT**

COUNTERMEASURE :

- An action, device, procedure, technique that reduces the **vulnerability** of a system or component is referred as **counter measure.**

OWNER:

1. Wish to minimise the risk by applying countermeasure.
2. Owner must value the assets he posses.
3. Owner must impose counter measure to reduce risk.

THREAT AGENT:

1. Threat agents give rise to threats,
2. That increase the risk IRO assets that may damage the system.

THREATS TO CYBER CRIMES:

In my notes, I already provided the short form of S.O.F.T. **D**.E.V., in which one point of denial of services included. As per amended ICAI material:

"An action or services that **prevent access to a software system** by its authorised users or **cause the delay of critical operations or prevent** any part of the system from functioning is termed as **"DoS".**

RISK MANAGEMENT:

RISK MANAGEMENT is process of identifying vulnerabilities & threats to the information resources used by an organisation in achieving business objectives & **deciding what countermeasure** to take in reducing the risks.

Now the question arises how to do risk management effectively. Following is the procedure or I would rather say it as benchmarks that helps in evaluating the risk. Following are the steps:

A. Understanding risk appetite of the entity.

B. On this basis **future investment in technology, extent to which IT assets to be protected etc** is decided by the management.

C. Next step is to **identify, analysis, evaluating, treating, monitoring & communicating** impact of the risk on IT processes.

D. After knowing risk appetite & doing risk assessment, clarified risk managing strategies can be formulated.

E. After all this it is up to management that whether it want to **avoid, mitigate, transfer or accept** the risks.

In this topic no further addition is there.

TECHNIQUES OF RISK EVALUATION:

"**DELPHI TECHINQUE**"

It is a method for structuring a group communication process, so that process is effective in allowing **group of individual** as a whole to **deal** with a complex problem.

RISK MITIGATION:

One question that arises that why we are doing the risk assessment and analysis. All this is done to mitigate the risk.

"**Risk Mitigation**" : Systematic reduction in the extent of exposure to risk/ likelihood of its occurrence.

"**Common Risk Mitigation Techniques**"

A risk mitigation strategy is an **organisational plan** for **"how it will address its identified risks".** In order to protect the organisational information assets, use of such risks mitigation strategies are very effective and cost effective too.

Some of the **risk mitigation measures are:**

- **S**elf assessment.
- **I**nsurance.
- **R**isk management department to be set up.
- **C**reating culture supportive of risk mitigation.
- **O**utsourcing operations with strict service level agreements.
- **L**imit of operational risk to be set up.
- **D**isaster Recovery Plan & backup system to be established
- **R**eserves calculating & capital requirements.

Chapter 8

INFORMTION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

IS 27001: INFORMATION SECURITY MANAGEMENT STANDARDS

It is international best practice and standard for information security management systems (ISMS). It is a systematic approach to manage **confidential or sensitive information.**

ISO defines how:

- Organise information security in any kind of information.
- **ISMS --** foundation of information security management.

ISMS define how to manage information security through a system of information security management. It consists of **4 phases** that should be implemented in order to minimise the risks:

Step 1: THE PLAN PHASE

- Plan the basic organisation of information security,
- **Set objective** & choose appropriate security controls.

Step 2 : THE DO PHASE

- Carrying out everything that was planned during the plan phase.

Step 1 : THE CHECK PHASE

- Monitor the functioning of ISMS through various "channels " &
- Check whether the result meets the set objectives.

Step 1 : THE ACT PHASE

- Improve everything that gone wrong in the previous phase.

These 4 phases is never ending process and to be **implemented cyclically** in order to have effective ISMS.

Now contents of each phase:

THE PLAN PHASE	THE DO PHASE
-- Scope of ISMS. -- Writing Policy for ISMS -- Risk assessment methodologies. -- Identify assets, threats, vulnerabilities -- Identifying risk size. -- Selection of controls for risks. -- Management approval for residual risk -- Mgmt. Approval of ISMS implementation	-- Writing risk treatment plan -- I.e. describes who, when, budget etc -- Implement risk treatment plan. -- Carry out awareness & training -- Managing normal operation of ISMS -- Management of ISMS resources
THE CHECK PHASE	**THE ACT PHASE**
-- Implementation of controls. -- Review of effectiveness of ISMS -- Internal audits at planned intervals. -- Update security plans. -- Keep records of the activities & incidents that may affect ISMS effectiveness.	-- Implementation of improvement in ISMS -- Take corrective & preventive controls -- Communicate activities & improvements To all stakeholders. -- Improvements led to goals achievement.

OTHER STANDARDS RELATED TO INFORMATION SECURITY

In addition to ISO 27001(Formerly BS 7799-2), ISO 27002(Formerly ISO 17799), is an auxiliary standards which provide more details on how to implement security controls specified in ISO 27001.

ISO 27005 : **Describes risk assessment procedures** in more detail.

BS 25999-2 : **Detailed description of business continuity management.**

AREAS OF ISMS FOCUS:

ISMS is a **set of policies** that is concerned with information security management or IT related risks. The logic or intention behind an ISMS is that organisation should formulate such set of policies in order to manage risks to its information assets.

There are 10 focus areas that is already explained in my notes with the short form SOAP PC AS BC.

CAPABILITY MATURITY MODEL:

SEI (Software Engineering Institute) + Mitre Corporation → **Developed CMM model**

CMM Presents:

- Sets of recommended practices in number of key process areas that have been shown to enhance software process capabilities.
- It is based on the knowledge acquired from software process assessment & feedback from the government and industry.
- A mature organisation clearly defines **procedures for software development** and **project management.** These procedures are adjusted & perfected.

There are 5 levels according to SEI:

1. **Initial :** Starting point for use of a new or undocumented repeat process.
2. **Repeatable :** Process is at least documented sufficiently.
3. **Defined :** Process is defined as standard business process & decomposed.
4. **Managed:** The process is managed in accordance with agreed upon metrics.
5. **Optimising :** Process management includes deliberate process improvement.

COBIT – IT GOVERNANCE MODEL

COBIT : Allows managers to **grip between control requirements, technical issues and the business risks.** It emphasis on regulatory compliance, helps entity to increase value attained from IT.

- **COBIT 5** is latest edition of ISACA(Information System Audit & Control Association)
- **Released in April 2012.** The principle in COBIT 5 embraces thoughtful leadership, and guidance from business, IT and governance experts around the world.
- **COBIT 5** is the business framework for the governance and management of enterprise IT.

1. Now a question arises that *WHY COMAPNY NEEDS or USE COBIT:*

- Enterprise needs good, reliable, repeatable data on which they can take good business decision.
- COBIT 5 is made and is customised to suit all the enterprises irrespective of their size, industries and geographical areas
- COBIT 5 provides enterprises a tool necessary to understand, utilise, implement and direct important IT related activities.
- COBIT 5 is intended to deliver business benefits to enterprises:
  - Increased use of IT experts, user satisfaction, less IT related risks etc.
  - Development of IT related business solutions.
  - Increased enterprise wide involvement in IT related activities.

2. Benefit of *COBIT 5:* **CODE TO REMEMBER : Q - T.R.I.C.**

- **Q**uality information is maintained to support business decision.
- Optimise cost of IT services & **T**echnology.
- Maintain IT related **R**isk at an acceptable level.
- Usage of **IT** to achieve operational excellence.
- **C**ompliance with relevant laws, regulations, agreements and policies.

3. *INTEGRATING COBIT WITH OTHER FRAMEWORKS:*

It is based on an enterprise view and is aligned with governance best practices:

- ❖ GEIT — This fourth edition of the IT Governance Institute's status report of the governance of enterprise IT covers 21 countries and 10 industries. It reveals accord on the contribution of IT to business success, the challenges and opportunities connected with IT the impact of the economic crisis and views on IT outsourcing, social networking.

- ❖ ITIL — The **Information Technology Infrastructure Library** (**ITIL**) is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business

- ❖ TOGAF — **The Open Group Architecture Framework** (TOGAF) is a high level and holistic approach to design, which is modeled at four levels: **Business, Application, Data, and Technology**. It aims at giving a well-tested overall starting model to information architects, which can then be built upon. It relies heavily on modularization, standardization and already existing, proven technologies and products.

- ❖ ISO 27000 — The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS). It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs

IMP : No need to remember the explanation to above said best practices.

4. *CUSTOMISING COBIT AS PER NEEDS:*

COBIT 5 can be tailored to meet the enterprise's need. Because of its open design, it can be applied to meet needs related to:

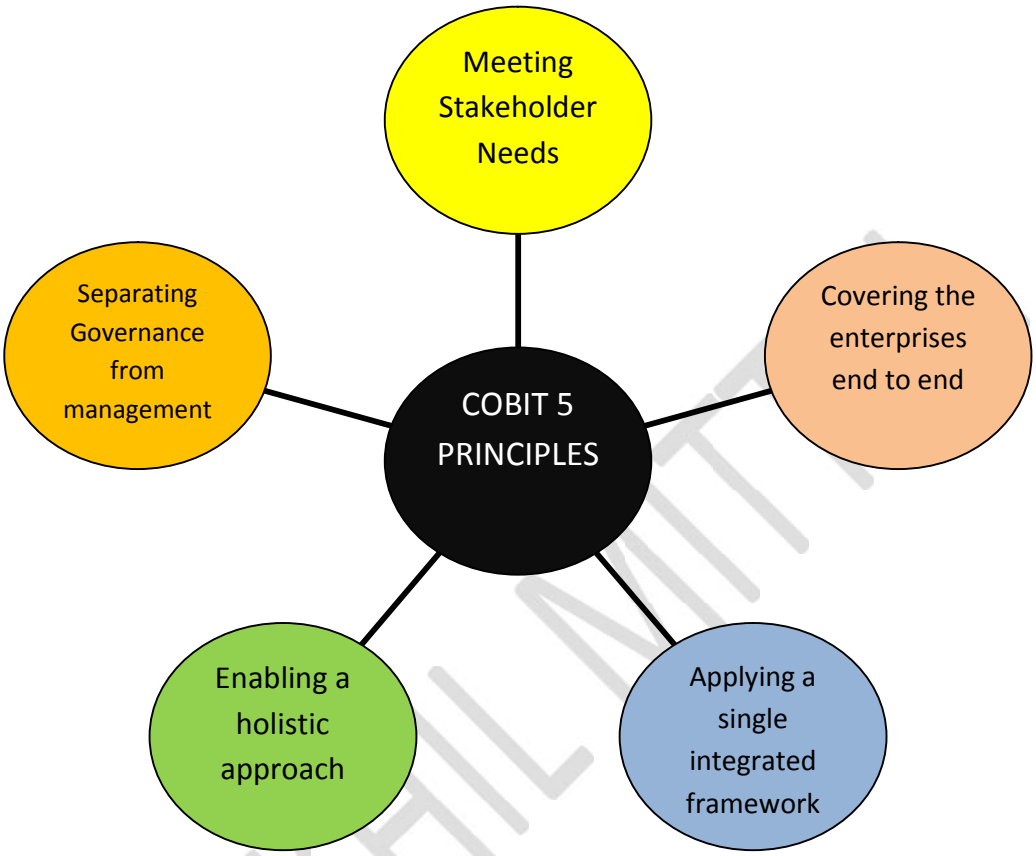
-- Information security -- Assurance Activities

-- Risk Management -- Governance & Management of enterprise IT

-- Financial Processing -- Legislative & regulatory compliance

5. *FIVE PRINCIPLES OF COBIT:*

❖ There are 5 key principles for governance & management of enterprise IT ,



Now explaining each of the steps in detail:

1. Meeting Stakeholder Needs:

❖ Enterprise exists to create value for their stakeholders, by maintaining balance,

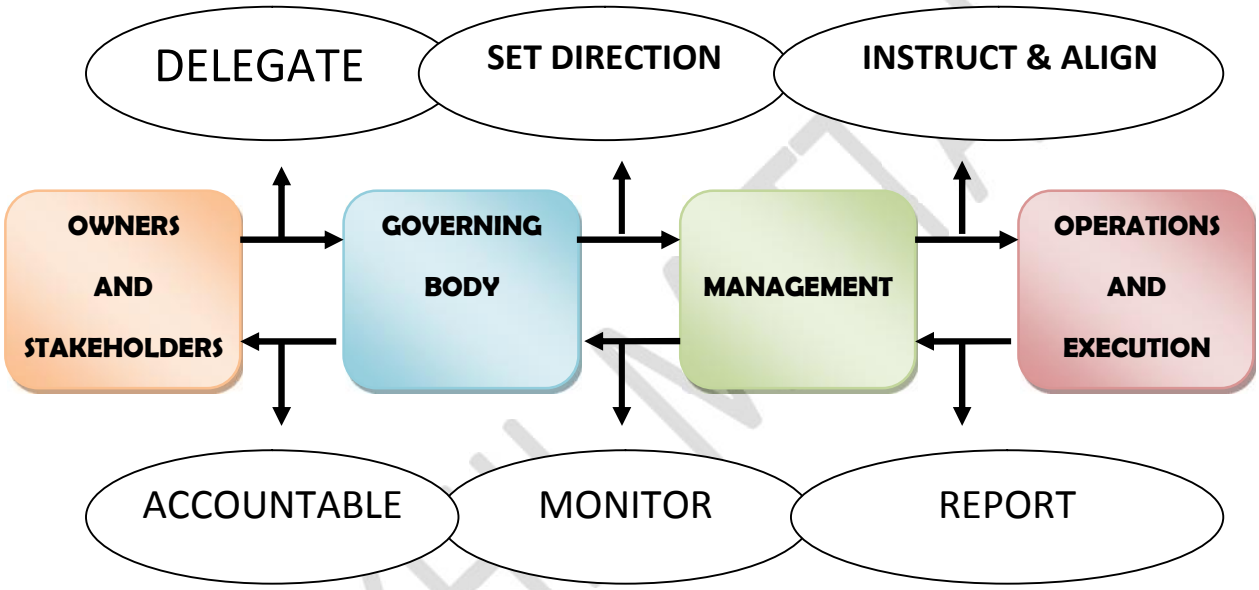
❖ Between **benefit realisation** & **risk optimisation.**

❖ COBIT 5 enables the enterprises to create such value by using COBIT processes.

❖ Since it is tailor made, as such an enterprise can easily modify it as per its requirement.

2. Covering enterprise End-to-End:

- ❖ It covers all functions & processes within the enterprise.
- ❖ COBIT 5 doesn't focus on IT function but treats information as an asset that need to be dealt with just like any other asset.
- ❖ It considers all in the enterprise whether internal or external that is relevant to governance & management of enterprise information and related IT.



3. Applying a single Integrated Framework:

- ❖ Since COBIT 5 can be integrated with other standards & frameworks,
- ❖ It is a single integrated framework that enables complete company coverage, providing a basis to integrate effectively other frameworks.

4. Enabling a holistic(Relating to or concerned with wholes or complete systems **) approach:**

- ❖ Effective governance of enterprise IT requires holistic approach.
- ❖ COBIT 5 defines a set of enablers to support the implementation of governance and management system for enterprise IT.

5. Separating Governance from management:

❖ COBIT 5 makes a clear distinction between governance & management.

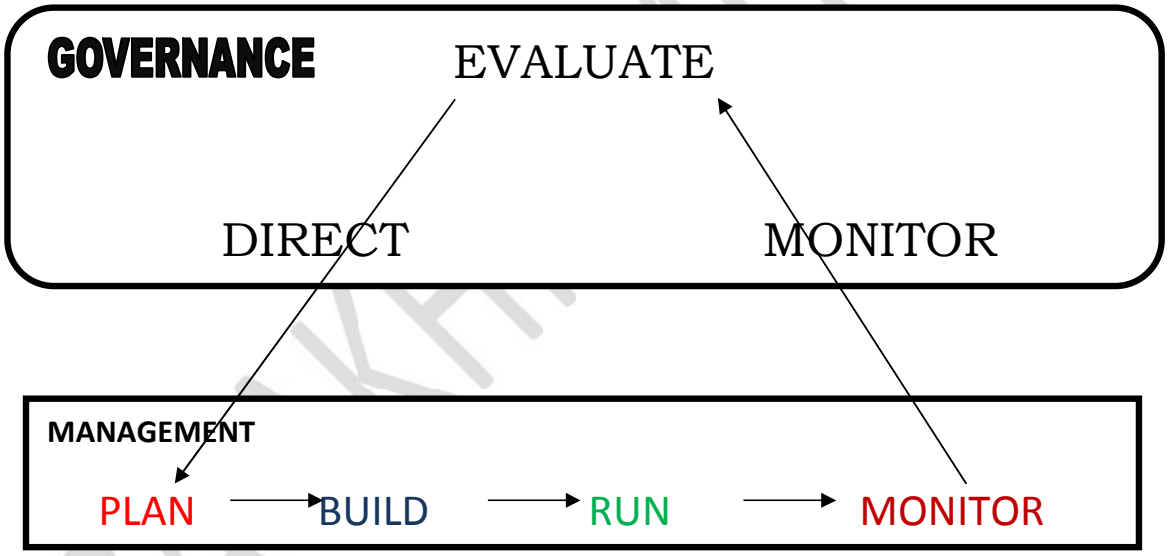
GOVERNANCE

Ensures that stakeholder **needs, conditions & options** are evaluated to **determine BALANCED, objectives** to be achieved, setting direction, through **decision making** & **monitoring.**

GOVERNANCE is responsibility of the BOARD OF DIRECTORS under the CHAIRPERSON.

MANAGEMENT

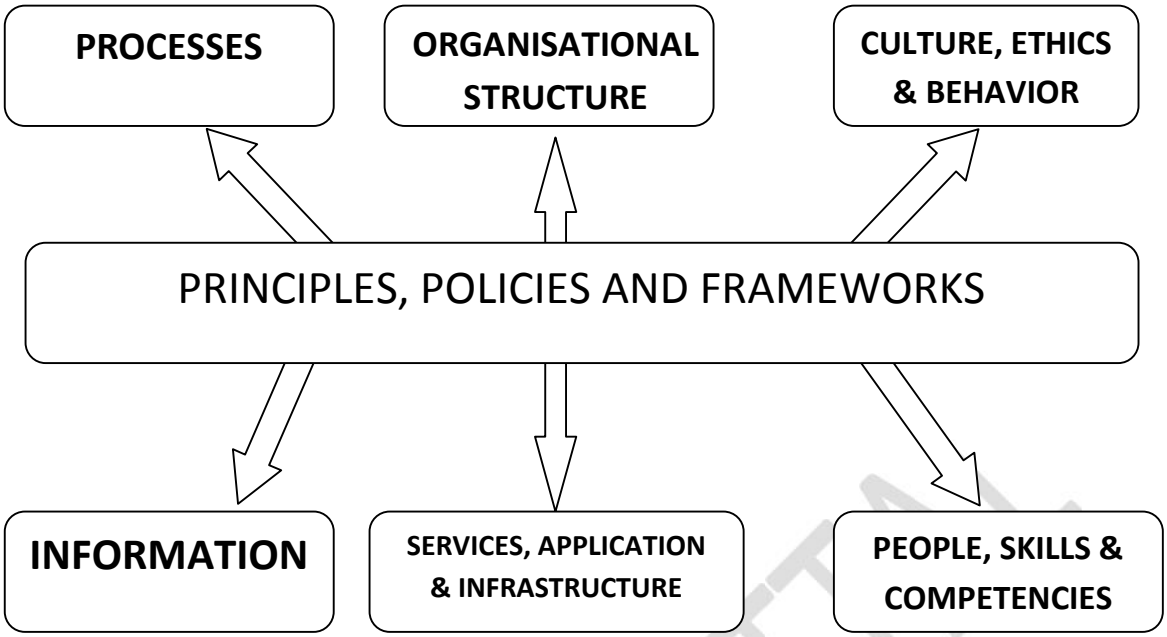
Plans, builds, run and monitor **activities** in alignment with the direction set **by the governance body** to achieve organisational objectives.



4. COBIT 5 ENABLERS:

Enablers are the factors **that collectively and individually influence** whether something **will work. Enablers** are driven by the **GOALS.** The COBIT 5 framework describes **7** categories of the enablers:

In Hindi, I would rather say factors ko क्या हासिल करना चाहिए for a good governance.



To remember: In **organisation structure** there are **people with skill & competencies that** use **information** to introduce **principles, policies & framework** in the processes so that there exists good **culture, ethics & behaviour.** After all this, company can provide quality **services, infrastructure & applications.**

1. **Organisational Structure:** This is the key **decision making** entities in the enterprises.
2. **People with skill & competencies:** All this required for successful completion of all activities and for making correct decision.
3. **Information:** It is needed at all level of management. It is required to keep organisation running and well governed.
4. **Principles, policies & framework:** These are the vehicle to translate desired goals into practical guide for day-to-day operations.
5. **Culture, ethics & behaviour:** Of individuals & enterprises is important part for the governance & management activities.
6. **Services, infrastructure & applications:** This provides company information technology processing and services.

5. COBIT 5 PROCESS REFERENCE:

COBIT 5 includes a process reference that describes in detail **a number of governance and management processes.** Characteristics:

- ❖ It represents all processes normally found in the enterprise IRO IT activities.
- ❖ Proposed process model is **complete, comprehensive model.**
- ❖ Each enterprise has different processes to achieve common goals.
- ❖ Good governance depends on **common language** usage for all parts of enterprise involved in **IT activities.**

CoCo : CRITERIA OF CONTROL

BACKGROUND: **Published** in **1995** by **Canadian Institute of Chartered Accountants.**

Following are the CHARACTERISTIC of CoCo:

1. CoCo is user friendly.
2. It describes internal control as action that promotes the best result for organisation.
3. **CoCo** is not a mean (way) of "**prescriptive minimum requirements**" but also "**useful in decision making**".

OBJECTIVES **of CoCo:**

1. Effectiveness & Efficiency of operations.
2. Reliability of internal & external reporting.
3. Compliance with applicable laws, regulations & internal laws.

ITIL : IT Infrastructure Library

MEANING:

-- It is set of practices for IT Service management (ITSM),
-- That focuses on aligning IT services with the business needs.
-- ITIL describes **procedures, tasks and checklists** that are not organisation specific.
-- Following are the details of ITIL framework:

Service Strategy	Service Design	Service Transition	Service Operation	Continual Service Improvement

Now explaining each framework in detail:

1. **SERVICE STRATEGY:**
   - ❖ Deals with strategic management approach for IT service management.
   - ❖ It provides guidance on leveraging service management capabilities to deliver effective services to customers.
   - ❖ Provide **guidance** on **design, development & implementation** of service mgmt.
   - ❖ Assisting organisation to position itself to deal with costs & risks associated.

2. **SERVICE DESIGN:**
   - ❖ Translate strategic plans & objectives & creates designs and specifications,
   - ❖ Provide guidance on design & development of service & service mgmt processes.
   - ❖ Service design can be extended to both new & existing services.

3. **SERVICE TRANSITION:**
   - ❖ Provide guidance on service design & implementation, and ensures services are being maintained effectively.
   - ❖ **Service Transition Volume** provides guidance on development & improvement of capabilities for transitioning **new & changed** services into operations.
   - ❖ Provide guidance on transferring control of services between customers & service providers.

4. **SERVICE OPERATION:**
   - ❖ Provide guidance on management of a service through its day to day production life.
   - ❖ Provide support to operations by means of new models & architectures.
   - ❖ Provide detailed **guideline** on processes, methods and **tools** in addressing control prospective.

5. **CONTINUAL SERVICE IMPROVEMENT:**
   - ❖ Provide guidance on measurement of service performance through service life cycle,
   - ❖ Suggesting improvements to ensure that service delivers maximum benefit.
   - ❖ Provides guidance on **linking improvement efforts** and outcomes with service strategy, design, transition, focusing on efficiency increase etc.

----------END----------