Aim

To equip students with the knowledge of governance in information security and the importance of information system development and planning

Instructional Objectives

After completing this chapter, you should be able to;

- Describe the purpose and scope of policies and procedures in governance
- Categorise policies
- Differentiate between policies and procedures
- Explain manual organisation in policies

Purpose and Scope of Policies and Procedures

Policies and Procedures in Governance

Policy and Procedures tell us how activities are performed in a functional area.

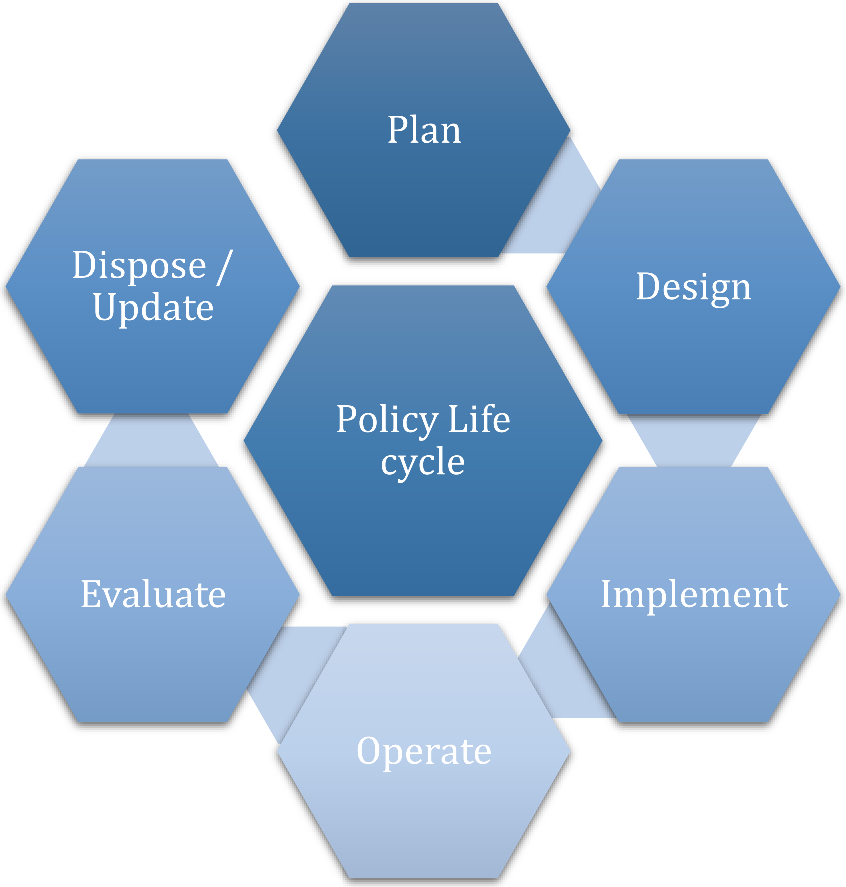
Privacy is a very important aspect and so is IT Policy.

A framework that allows the policies and procedures of a company to be structured in a logical manner is a policy framework.

Policies are building blocks for good governance and management of IT.

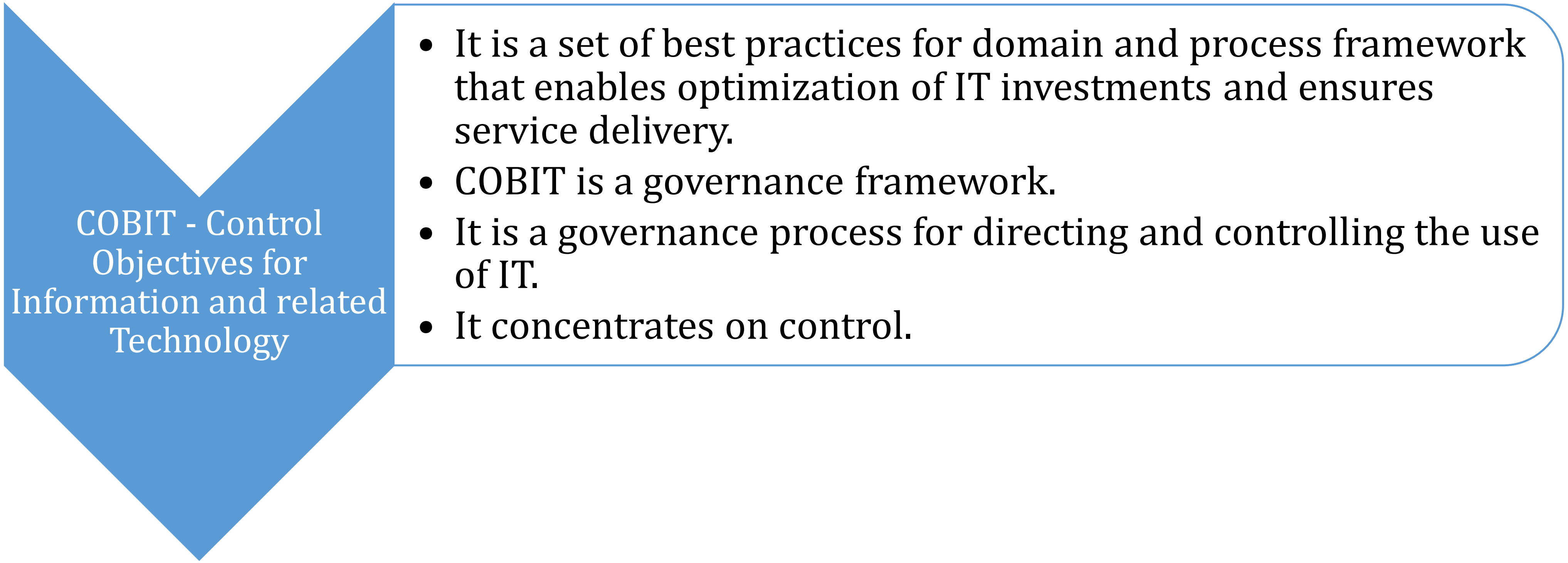
Policies are required to cover aspect of the internal control system of the organization to abide by the legal and business requirements.

Life cycle of Policies



The Policy Lifecycle

Purpose and Scope of Policies and Procedures in Governance

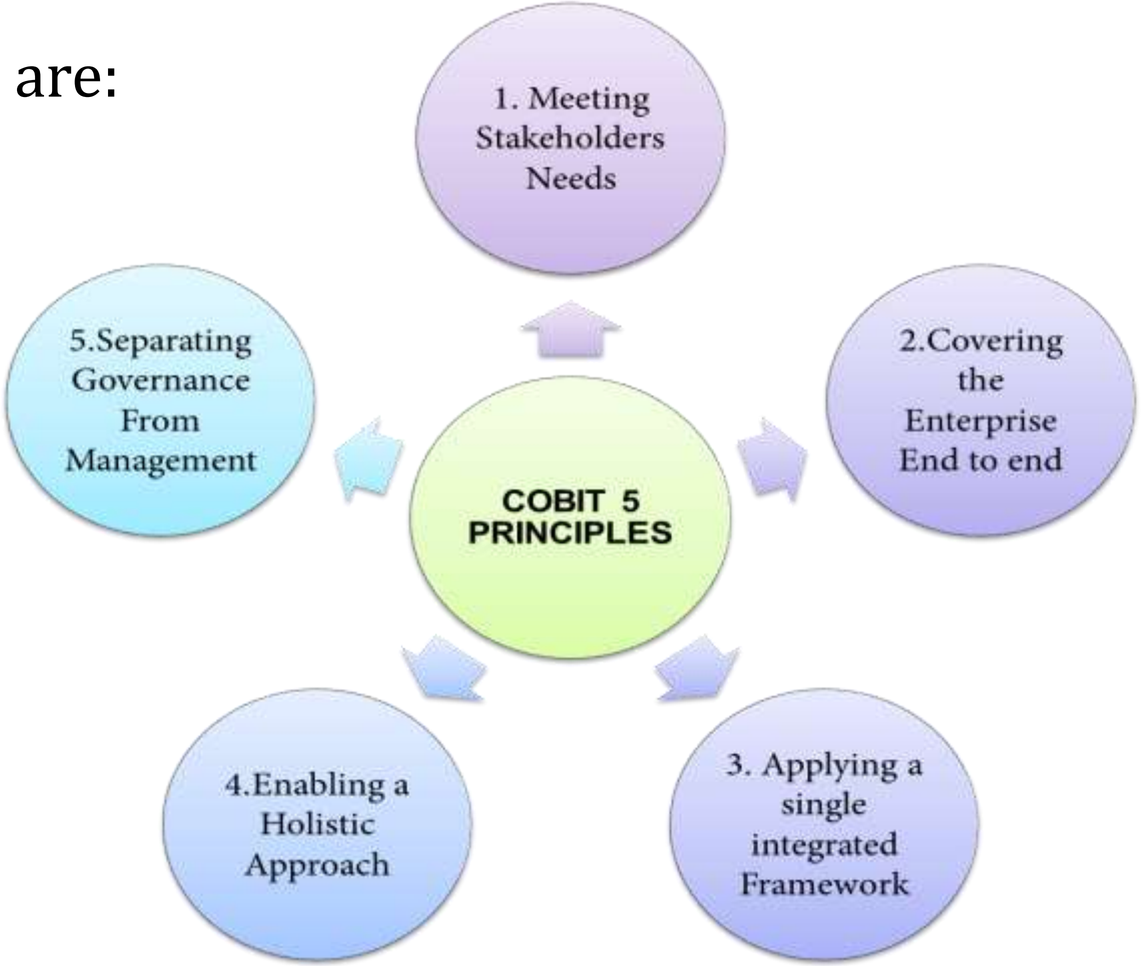


COBIT - Control Objectives for Information and related Technology

- It is a set of best practices for domain and process framework that enables optimization of IT investments and ensures service delivery.
- COBIT is a governance framework.
- It is a governance process for directing and controlling the use of IT.
- It concentrates on control.

Purpose and Scope of Policies and Procedures in Governance

The 5 principles of COBIT are:


COBIT 5 PRINCIPLES
1. Meeting Stakeholders Needs
2.Covering the Enterprise End to end
3. Applying a single integrated Framework
4.Enabling a Holistic Approach
5.Separating Governance From Management

Principles of COBIT

Quiz / Assessment

1) What is an building block for good governance and management of IT?

a) Planning
b) Policy
c) Production
d) Putrefaction

Quiz / Assessment

2) What is a governance process for directing and controlling usage of IT

a) COBIT

b) COBOL

c) COBRA

d) ARBCO

Quiz / Assessment

3) Expand this acronym - 'COBIT'

a) Cobra orbital broadband information system

b) Commando over the sky broadband radio transmitter

c) Control Objectives for Information and related Technology

d) Controller based arduino pie making technology

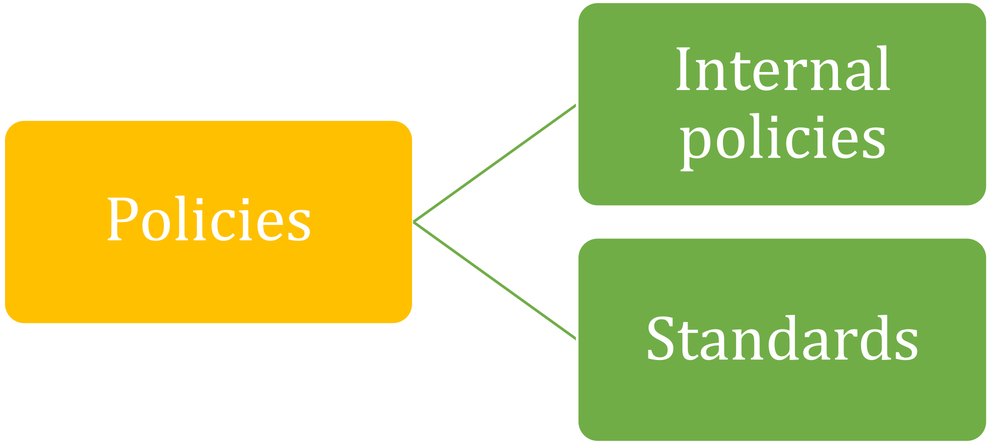
Categorise Policies

Types of Policies

A Policy is a high level document created or developed by the management to convey the driving strategy to its employees.

There are 2 types of policies. They are Internal policies and standards

Standards: Any external standard such as ISO 9001:2015 is an example of a standard policy



Policies

Internal policies

Standards

Types of Policies

Policy Development

Policies can be created in two ways:

- Top Down Approach
- Bottom Up Approach

Regulatory

Advisory

Informative

Quiz / Assessment

4) What is meant by a ‘Policy’?

a) It is a high level document created for high level purpose

b) It is a high level document developed by the management to convey the driving strategy

c) It is a high level document created by high level people

d) It is a high level document created by the Police department

Quiz / Assessment

5) By what approaches are policies created?

a) Top Down and Bottom Up Approach
b) Lateral left and peripheral right side Approach
c) Top top and bottom Approach
d) Stick and Buffalo ownership approach

Quiz / Assessment

6) What is covered under the 'Security policy'?

a) CAD/CAM operation safety and security mechanism
b) Machine fencing and safety grill assembly
c) Usage, operation and security of information system and assets
d) Locks, safes and strong rooms containing company's money

Differentiation between Standards, Policies and Procedures

Differentiation between Standards, Baselines and Guidelines

Standards

- They are more specific than a policy. And are tactical documents that outlay the steps for a process.

Baselines

- A baseline is a minimum threshold level a device, system or network element has to adhere to.
- Though passwords can be longer, the minimum threshold level is 8 characters. These baselines generally map to regulatory or industry standards.

Guidelines

- These are the Best Practices to follow for a particular process or procedure.

Quiz / Assessment

7) What is meant by a 'Standard'?

a) A standard is a tactical document outlining the steps to be followed for a process
b) It is a standardized document prepared following a standard step
c) It relates to the official flag and logo of the company
d) It is a formal rule and guideline to be followed by all

Quiz / Assessment

8) What is meant by a 'Baseline‘?

a) It is used in measuring the base of a given location

b) It is a minimum threshold level of adherence applicable to a device, system or a network element

c) It measures the distance one must run, while playing baseball

d) It measures the safe length of depth while BASE jumping

Quiz / Assessment

9) What is meant by a ‘Guideline’?

a) It comes into picture while guiding people across a line

b) It refers to the best practices to be followed for a particular process or procedure

c) It helps student while studying by guiding them across difficult questions

d) It helps linemen in repairing electricity lines

Manual Organization in Policies

Manual organisation in policies

Policy manuals are developed to help the employees and organisation teams run the organization.

Every chapter in the manual is a subject area where all the related policies are placed.

A manual is not intended to be read from the start up till the end. It is referred to only when required.

Hence it is necessary to provide proper naming convention and indexing.

Quiz / Assessment

10) __________ are developed to help the employees and organization teams in running the organization

a) Policy manuals

b) Police manuals

c) Politics manuals

d) Polite manuals

Quiz / Assessment

11) There is no need to read a manual completely. One can refer it when it is required. True or false?

a) The statement is true

b) The statement is false

Quiz / Assessment

12) Which tool is used for cross-referencing and mapping purpose between various policies, standards and templates?

a) Tally tool
b) Paxel tool
c) Excel tool
d) Word tool

Quiz / Assessment

1) Describe the 5 principles of COBIT 5.
2) What are the various steps involved in implementing an IT policy framework using COBIT 5?
3) Design an IT User Management Procedure document for SOLO Cup based on the content provided in this chapter.
4) Differentiate between COBIT 4.1 and 5.0.

Activity

Online Activity
(45 min)

- Description: Perform an online research on policies and procedures of IT governance and prepare a presentation of (20 slides)

Note: Refer Table of Content for the activities

Summary

- ✓ The primary objective of IT Governance is to protect the interest of the shareholder and also being transparent about the enterprise risks.
- ✓ The strategy document of a company reflects the management's view of the company.
- ✓ A Policy is a high level document created or developed by the management to convey the driving strategy to its employees.
- ✓ Policy and procedures share a parent-child relationship. If Policy is the parent, procedure is the child.
- ✓ COBIT stands for Control Objectives for Information and related Technology. Currently it is in its fifth version.
- ✓ It is a governance framework that helps in managing an enterprise in a comprehensive manner covering all the business and functional areas while considering the IT investments and interests of the stakeholders.
- ✓ One of the very important steps in IT Governance, is to develop a policy and procedures manual; be it a hard copy version or an online version.

e-References

- Ptgmedia. *IT Governance*. from http://ptgmedia.pearsoncmg.com/images/9780789735737/samplechapter/0789735733_CH02.pdf
- Isaca. *IT Policy FrameworkBased on COBIT 5.* from http://www.isaca.org/Journal/archives/2013/Volume-1/Pages/IT-Policy-Framework-Based-on-COBIT-5.aspx
- Isaca. *COBIT Case Study: Solo Cup Uses COBIT to Develop IT Policies.* from http://www.isaca.org/knowledge-center/cobit/pages/cobit-case-study-solo-cup.aspx
- Books. *IT Governance Policies & Procedures*. from https://books.google.co.in/books?id=8jBYCwAAQBAJ&pg=SA6-PA5&lpg=SA6-PA5&dq=manual+organization+IT+Governance&source=bl&ots=KEdv86YdC-&sig=ExMYoYg3Y1qx7TB04mOcaGSd5rk&hl=en&sa=X&ved=0ahUKEwihgNT8luPLAhUUBo4KHRApA24Q6AEIRTAH#v=onepage&q=manual%20organization%20IT%20Governance&f=false

External Resources

1. Weill, Peter, &Ross, Jeanne. (2004). *IT Governance* (1 ed.). Boston: Harvard Business School Press.