Chapter 4.2

Information Security Frameworks

Aim

To equip the students with the knowledge of different security frameworks

Instructional Objectives

After completing this chapter, you should be able to:

- Explain information security frameworks
- Elaborate on COBIT
- Describe COSO-ERM and SAS

Information Security Frameworks

Information Security Framework

IT Security frameworks are a set of processes that are used to define the IT Security policy and processes of an organization and the ongoing management of information security controls.

Quiz / Assessment

1) IT Security policy is defined by using a a set of process called ______________.

   a) IT Security frameworks
   b) IT System frameworks
   c) IT Strategy frameworks
   d) IT Standard frameworks

Quiz / Assessment

2) Which of the following is a direct benefit of using a security framework?

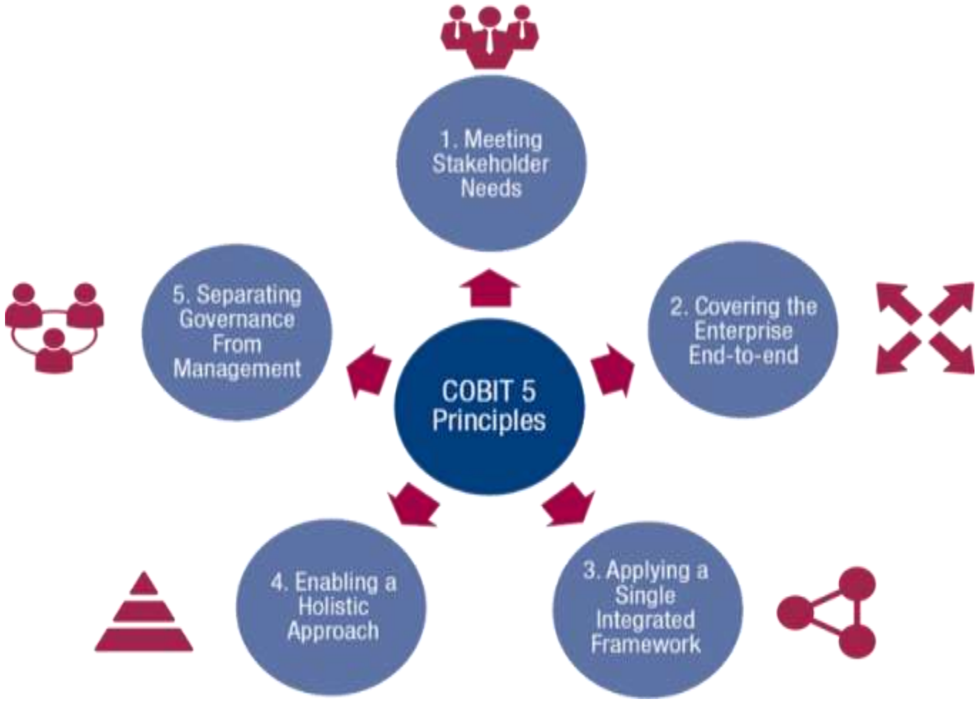
a) It helps in establishing a complete security program for the entire organization
b) It helps us to extract information that is of relevance amidst the chaos
c) It helps drive the enterprise value
d) It helps in creating value for the stakeholders manage the risks and reduce the vulnerabilities

Quiz / Assessment

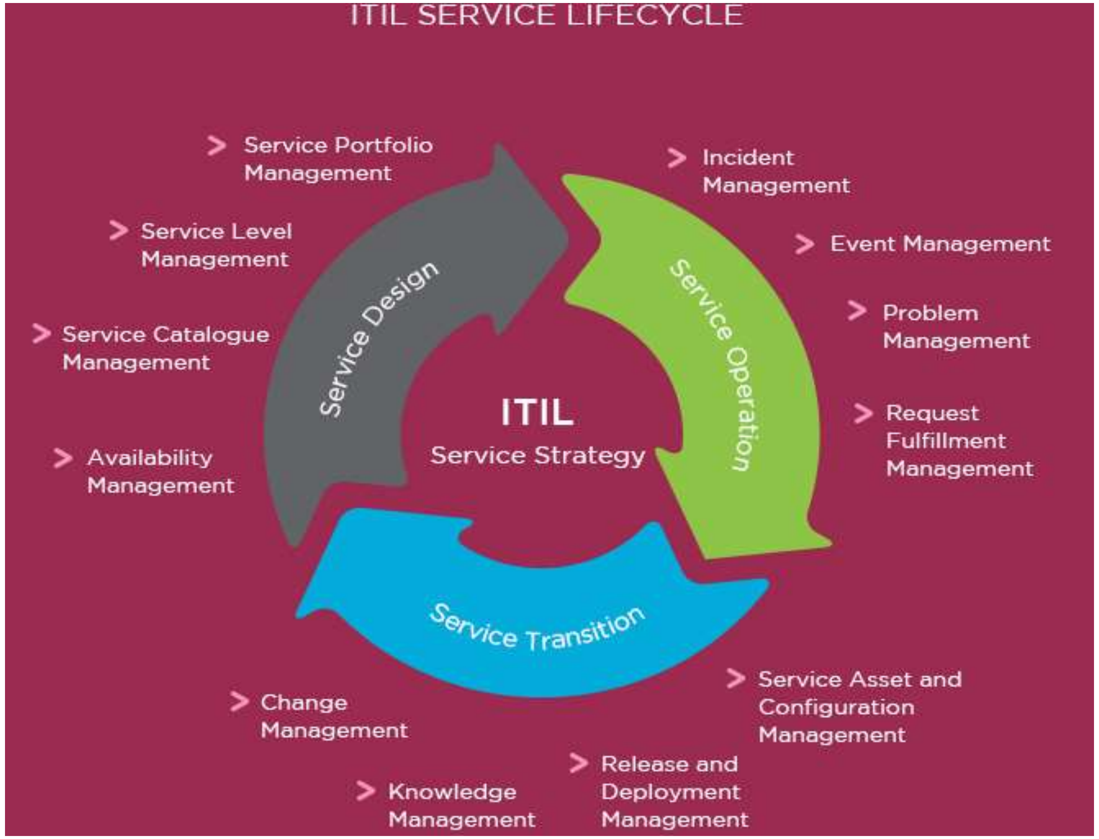
3) BSI-Standard-100-1 is a security framework. State true or false?
   a) True
   b) False

COBIT

Principles of Cobit 5.0


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
COBIT 5 Principles

Components of ITIL



ISO / IEC 27000 Series

- Scope of the standard
- How the document is referenced
- Reuse of the terms and definitions in ISO/IEC 27000
- Organisational context and stakeholders
- Information security leadership and high-level support for policy
- information security management system; risk assessment; risk
- Supporting an information security management system
- Making an information security management system operational
- Reviewing the system's performance
- Corrective action

Quiz / Assessment

4) Which of the following is not a COBIT principle?

a) Meeting Stakeholder needs
b) Covering the Enterprise end-to- end
c) Enabling a Holistic Approach
d) Enabling an innovative service design

Quiz / Assessment

5) ITIL stands for _______________.

   a) Information Technology Infrastructure Library
   b) Information Technology Initiatives Lab
   c) International Technological Institute for Linguistics
   d) International Testing Institute, Ludhiana

Quiz / Assessment

6) The five components of ITIL are ___________.

a) Service Statistics, Service Development, Service Design, Service Operations and Continual Service Improvement
b) Service Strategy, Service Design, Service Transition, Service Operations, Continual Service Improvement
c) Service Strategy, Service Design, Service Transition, Service Operations, Service Maintenance
d) Service Strategy, Service Knowledge Transfer, Service Operations, Service Maintenance and Service Design

Quiz / Assessment

7) ISO 27000 series of standards emphasises on measurement and performance of _______________.

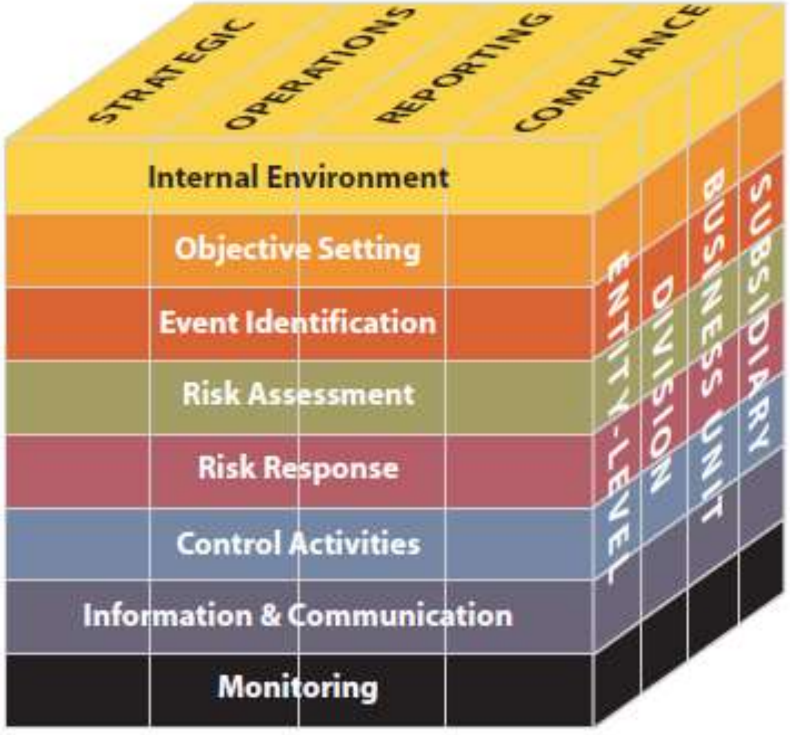
a) ISMS
b) Software System Development
c) Application Software Maintenance
d) System Requirements Gathering

COSO-ERM and SAS

Objectives of COSO-ERM

COSO’s Enterprise Risk Management – Integrated Framework

- It extends the Internal Control framework to include risk management practices.
- It does not replace the Internal Control Framework.
- It includes the Internal Control Framework completely in the ERM Integrated Framework.
- Hence, companies that adopt this ERM Integrated Framework can use the Internal Control Framework for the internal control practices and then continue to use ERM for the enterprise wide Risk Management System.



Quiz / Assessment

8) COSO is mainly intended at the following audience __________.

   a) Management
   b) Financial Auditors
   c) Information System Auditors
   d) Development Team

Quiz / Assessment

9) COSO ERMs objectives are classified into four categories and they are __________.

a) Strategic, Development, Operations, Maintenance
b) Strategic, Operations, Reporting and Compliance
c) Development, Operations, Reporting and Compliance
d) Development, Operations, Audit and Reporting

Quiz / Assessment

10)COSO ERM is ____________.

a) Encompasses COSO's Internal Control
b) Internal Control and ERM are two different topics that are unrelated
c) COSO ERM supersedes Internal Control
d) Is for Enterprise Resource Management where-as COSO's internal Control is for financial controls.

SAS

SAS

SAS 70 (Statement on Auditing Standards No. 70) was developed by American Institute of Certified Public Accountants.

SAS 70 defined the standards for an independent auditor to follow for assessing the internal controls of an organisation.

Since it is coming from an independent organisation, this certificate of compliance will provide the necessary trust of the customers.

Having a SAS audit done will provide the edge for the service organisation over its peers since its internal controls have been validated for effectiveness and compliance.

Quiz / Assessment

11) Which of the following is one of the inputs to the IS Strategic Plan?

a) Organizational Strategic Plan
b) IT Architecture
c) Target IT Landscape
d) IS operational plan

Quiz / Assessment

12) The main purpose of SAS is ___________.

a) To provide a risk management standard for the enterprise
b) To provide a IT governance framework for the enterprise
c) To provide a guideline for maximising the returns on IT investment
d) To provide an authoritative auditing standard

Quiz / Assessment

13)____________ defines the standards for an independent auditor to follow for assessing the internal controls of an organisation.

a) SAS 70
b) COSO ERM
c) ISO 9000
d) SSAE No. 16

Activity

Offline Activity

Offline Activity
(45 min)

- Prepare a presentation on COBIT (Minimum 10 slides)

Note: Refer Table of Content for the activities

Summary

- A set of processes that are used to define the IT Security policy and processes of an organization and the ongoing management of information security controls is called IT Security frameworks.
- In the mid-90s' Control Objectives for Information and Related Technology (COBIT) was developed by ISACA which is an independent organization of IT Governance professionals.
- COBIT principles are as follows:
  - Meeting Stakeholder Principles
  - Covering the Enterprise end-to-end
  - Applying a single integrated framework
  - Enabling a Holistic Approach
  - Separating Governance from Management

Summary

- A holistic integrated framework is required to satisfy both the needs of business and IT. COBIT 5.0 is aimed at achieving this. It enables organizations to implement IT Governance processes that can be audited and measured and hence can be continually improved upon.
- COBIT encompasses a number of frameworks such as ISO 27000, ITIL, COSO etc.
- The Committee of Sponsoring Organisations of the Treadway Commission (COSO) developed the “Internal Control – Integrated Framework” in the early 1990s. It was a guideline for companies to assess and enhance their internal controls.
- SAS 70 was replaced by Statement on Standards for Attestation Engagements – SSAE No. 16 in the year 2011.

e-References

- ISACA. *Cobit 4.1 Brochure.* Retrieved June 15, 2010, from http://www.isaca.org/knowledge-center/cobit/documents/cobit-4.1-brochure.pdf
- Qualified-audit-partners. *Cobit 5 ISACA's new Frame work for IT Governance, Risk, Security and Auditing.* Retrieved March 24, 2013, from http://www.qualified-audit-partners.be/user_files/QECB_GLC_COBIT_5_ISACA_s_new_framework_201303.pdf
- Searchsecurity. *COBIT.* Retrieved from http://searchsecurity.techtarget.com/definition/COBIT