University of Mumbai

M.Sc in Information Technology

Revised Syllabus 2019-2010

PSIT302 & PSIT3P2 – Information Security Management (ISM)

Dr. (Mrs.) R. Srivaramangai

Head, Department of Information Technology

rsrimangai@udit.mu.ac.in

Unit I – Security Assurance Approaches OCTAVE and COBIT

- The challenge enterprises face today is in adopting a robust, process-oriented information security risk assessment framework to comply with the control objective

OCTAVE

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE®)

- Approach that enables organizations to understand, assess and address their information security risks from the organization's perspective.
- OCTAVE is not a product, rather it is a process driven methodology to identify, prioritize and manage information security risks.

OCTAVE

It is intended to help organizations:

- Develop qualitative risk evaluation criteria based on operational risk tolerances

---

- Identify assets that are critical to the mission of the organization
- Identify vulnerabilities and threats to the critical assets
- Determine and evaluate potential consequences to the organization if threats are realized
- Initiate corrective actions to mitigate risks and create practice-based protection strategy

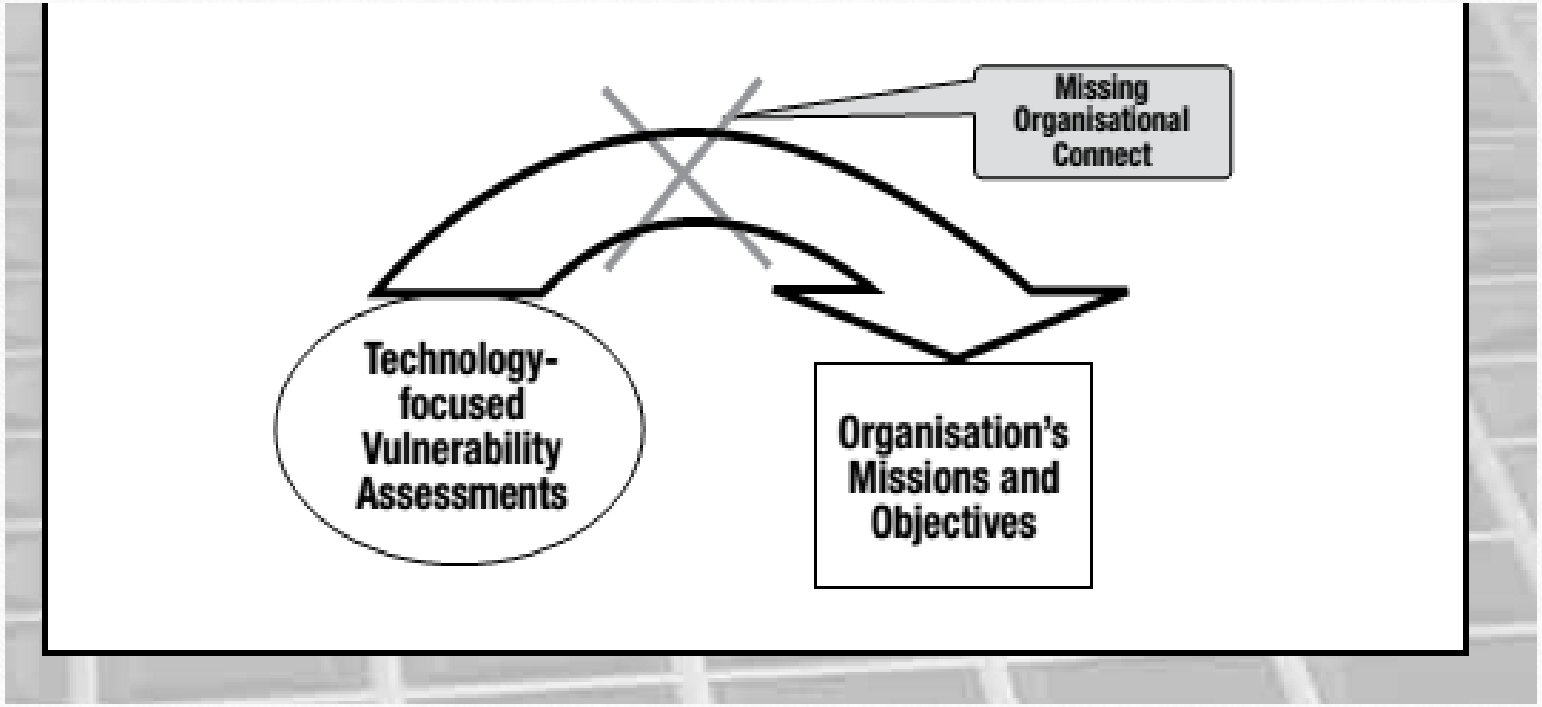
The OCTAVE approach was developed by the Software Engineering Institute (SEI) at Carnegie Mellon University to address the information security compliance challenges faced by the US Department of Defense (DoD). SEI is a US federally funded research and development centre sponsored by the DoD.

Why OCTAVE?

Determining Optimal Security

- For example, a health care company might consider its customers' records to be one of its important information assets. Likewise, a military establishment might consider its data on troop deployment to be an important information asset.
- Fail to establish the effect of the infrastructure weaknesses on information assets
- This leads to a gap between the organization's operational requirements and IT requirements.

Generic Approach to Security



What OCTAVE Gives?

- Managed by OCTAVE criteria comprising of principles, attributes and outputs.
- Principles are the fundamental concepts driving the OCTAVE evaluation process.
- Attributes are derived from principles and are the tangible elements, and outputs are the required results that must be achieved.
- There can be many methods to implement OCTAVE, but there is only one set of criteria with which all methods must be consistent.
- Organizations can develop methods that are consistent with the OCTAVE criteria or adopt any of the existing methodologies.

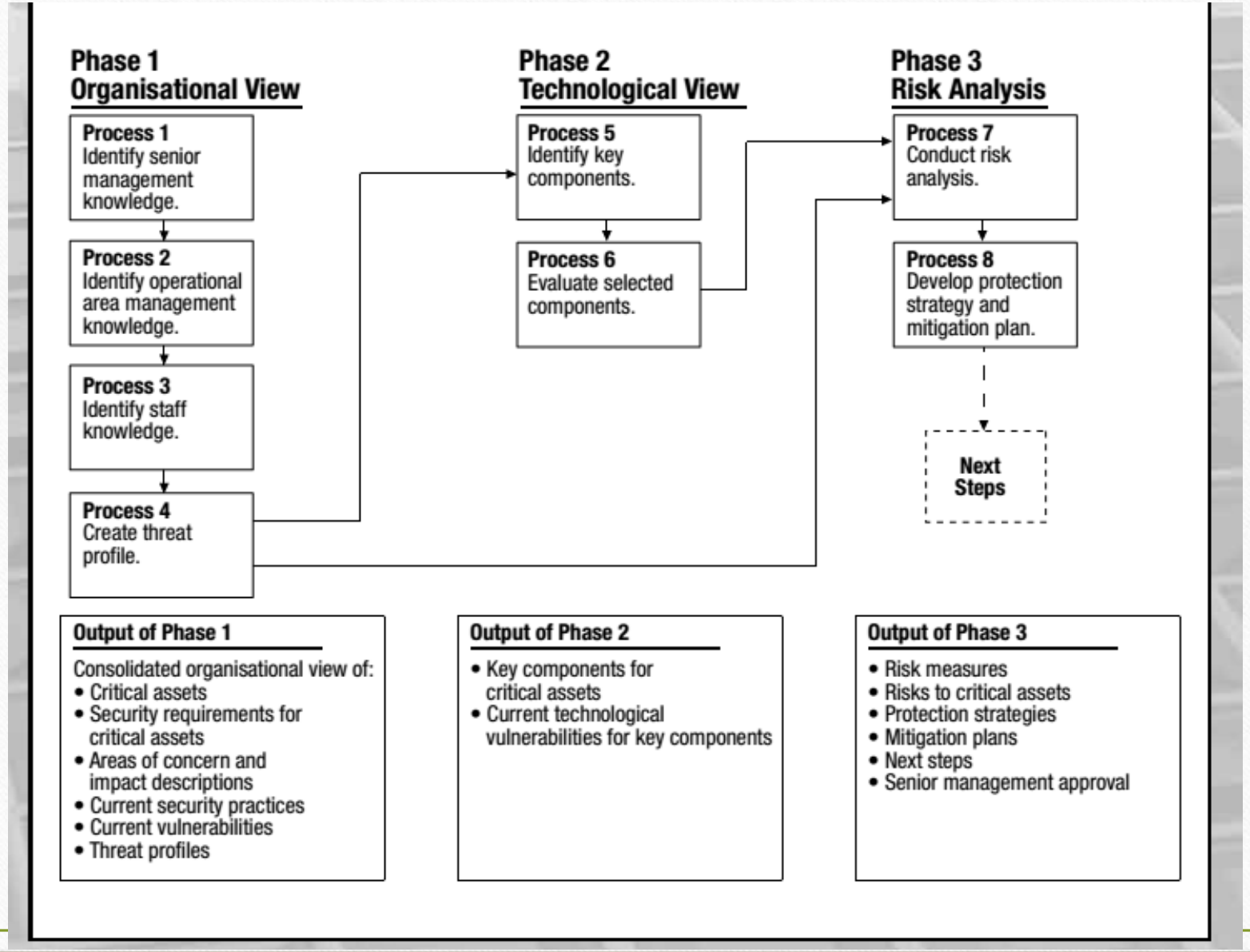
Evolution

Figure 2—OCTAVE Evolution	
Date	**Publication**
June 1999	OCTAVE Framework, Version 1.0
September 2001	OCTAVE Method, Version 2.0
December 2001	OCTAVE Criteria, Version 2.0
September 2003	OCTAVE-S, Version 0.9
March 2005	OCTAVE-S, Version 1.0
June 2007	OCTAVE Allegro, Version 1.0

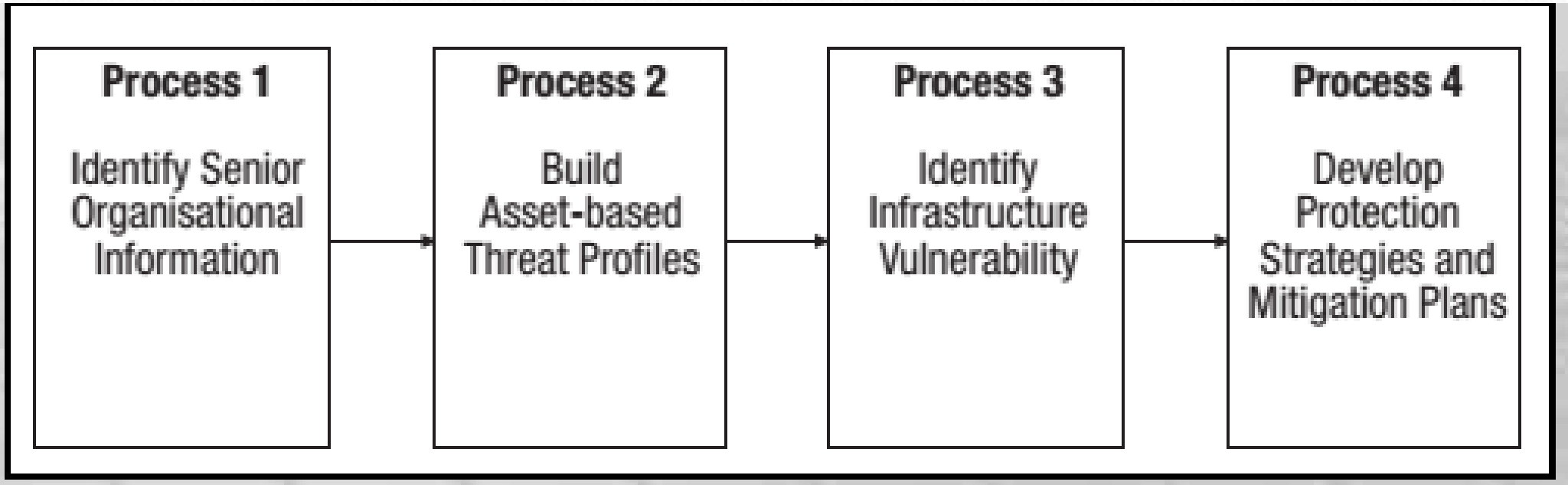
Analysis For OCTAVE

- When applying OCTAVE, a small team of people from the operational or business units and the IT department works together to form the analysis team and addresses the security needs of the organization. The analysis team:
  - Identifies critical information assets
  - Focuses risk analysis activities on these critical assets
  - Considers the relationships amongst critical assets, the threats to these assets and the vulnerabilities (both organizational and technological) that can expose assets to threats
  - Evaluates risks in operational context, i.e., how the critical assets are used to conduct the organization's business and how they are at risk due to security threats and vulnerabilities
  - Creates practice-based protection strategy for organizational improvement as well as risk mitigation plans to reduce the risk to the organization's critical assets

OCTAVE Method



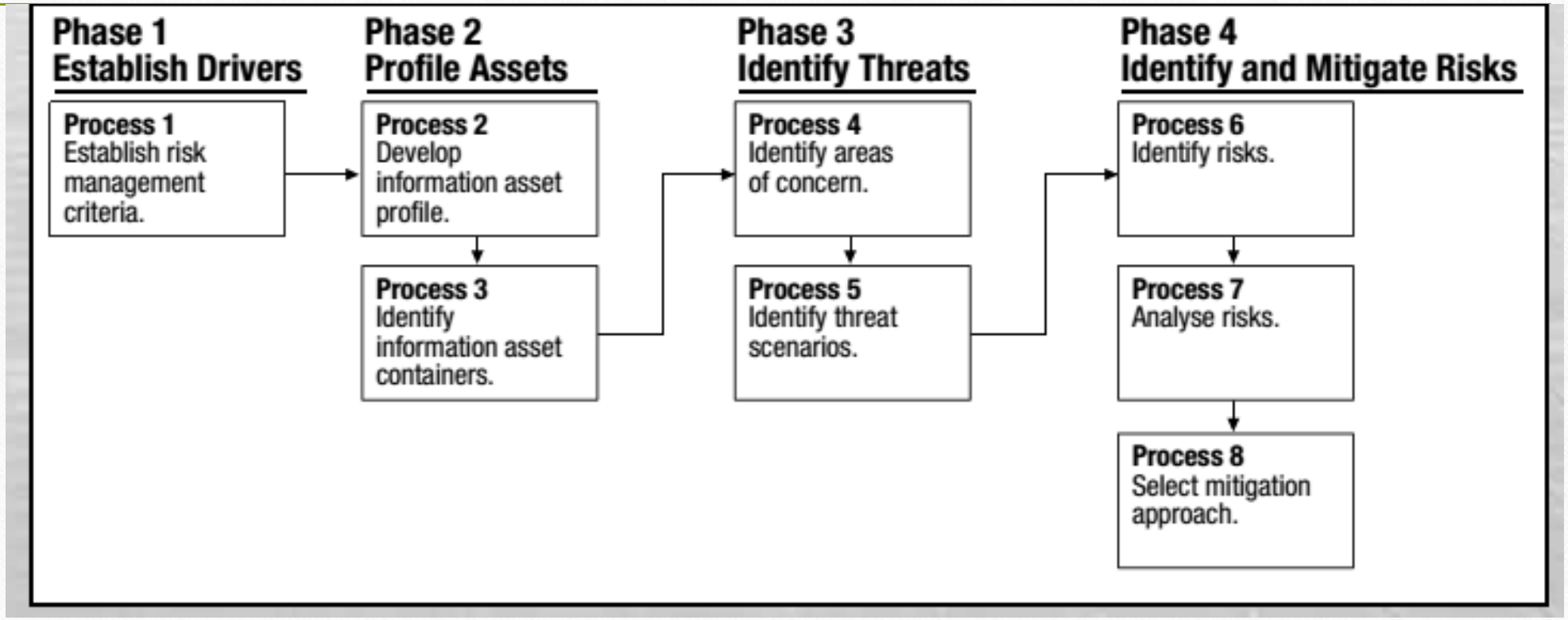
OCTAVE for Small Organizations
OCTAVE-S



OCTAVE Allegro

- Focused on risk assessment in an organizational context, but offers an alternative approach and attempts to improve an organization's ability to perform risk assessment in a more efficient and effective manner.
- Some key drivers that led SEI to formulating this new methodology include:
  - Improving ease of use
  - Refining the definition of assessment scope by introducing the container concept
  - Streamlining data collection and threat identification processes
  - Reducing training and knowledge requirements
  - Improving institutionalization and repeatability
  - Reducing the technology view

OCTAVE Allegro Process



Key success factors for OCTAVE

- Getting senior management sponsorship
- Selecting a champion and an analysis team to lead the evaluation
- Selecting the scope of evaluation
- Selecting participants for evaluation activities

Control OBjectives for Information and related Technology (COBIT)

- COBIT is just one of the frameworks from ISACA (Information Systems Audit and Control Association), an international professional association, affiliated member of (IFAC) International Federation of Accountants and (ITGI) IT Governance Institute.
- ISACA has more than 86,000 members in 160 countries and is a recognized worldwide leader in IT governance, control, security and assurance which was founded back in 1969.

COBIT

- COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
- COBIT enables clear policy development and good practice for IT control throughout organizations.
- COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework

COBIT's maturity model

Encompasses of the following levels:

- non-existent
- initial / ad hoc
- repeatable but intuitive
- defined process
- managed and measurable
- Optimized
- COBIT is made up of a number of "domains", "processes" & "activities"

DOMAIN and Processes

- DOMAIN 1
  - Plan & Organize (PO)
- PROCESSES
  - PO1 Define a Strategic IT Plan and direction
  - PO2 Define the Information Architecture
  - PO3 Determine Technological Direction
  - PO4 Define the IT Processes, Organization and Relationships
  - PO5 Manage the IT Investment (ITIL related: Financial Management for IT Services)
  - PO6 Communicate Management Aims and Direction
  - PO7 Manage IT Human Resources
  - PO8 Manage Quality
  - PO9 Assess and Manage IT Risks
  - PO10 Manage Projects

DOMAIN and Processes

- DOMAIN 2
  - Acquire & Implement (AI)

- PROCESSES
  - AI1 Identify Automated Solutions
  - AI2 Acquire and Maintain Application Software
  - AI3 Acquire and Maintain Technology Infrastructure
  - AI4 Enable Operation and Use
  - AI5 Procure IT Resources
  - AI6 Manage Changes (ITIL related: Change Management)
  - AI7 Install and Accredit Solutions and Changes (ITIL related: Release Management)

DOMAIN 3 - Deliver & Support (DS)

- PROCESSES
  - DS1 Define and Manage Service Levels (ITIL related: Service Level Management)
  - DS2 Manage Third-party Services
  - DS3 Manage Performance and Capacity (ITIL related: Capacity Management)
  - DS4 Ensure Continuous Service (ITIL related: IT Service Continuity Management)
  - DS5 Ensure Systems Security (ITIL related: Security Management)
  - DS6 Identify and Allocate Costs (ITIL related: Financial Management for IT Services)
  - DS7 Educate and Train Users
  - DS8 Manage Service Desk and Incidents (ITIL related: Incident Management)
  - DS9 Manage the Configuration (ITIL related: Configuration Management)
  - DS10 Manage Problems (ITIL related: Problem Management)
  - DS11 Manage Data (ITIL related: Availability Management)
  - DS12 Manage the Physical Environment
  - DS13 Manage Operations

DOMAIN and Processes

- DOMAIN 4
  - Monitor & Evaluate (ME)

- PROCESSES
  - ME1 Monitor and Evaluate IT Processes
  - ME2 Monitor and Evaluate Internal Control
  - ME3 Ensure Regulatory Compliance
  - ME4 Provide IT Governance

Uses of COBIT

- COBIT is intended for management, business users of IT and auditors:-
  - * managers = to balance risk and control investment, since these are the people who control and direct;
  - * users = who require assurances on security and control of IT services;
  - * auditors = structure and substantiate opinions as well as provide advice to managers to improve controls;
- Although ITIL (IT Infrastructure Library) is the dominant framework with regards to ITSM (IT Service Management), COBIT assists to further improve ITSM;
- Primary reason for COBIT benefiting management is to help balance risk and control investment decisions;
- COBIT's main aim is to address the business objectives