ISACA®

Trust in, and value from, information systems

Securing Sensitive Personal Data or Information in India

Using COBIT 5
For India's IT Act

2012 India Webinar Series

Presented by

Avinash W. Kadam
CISA, CISM, CGEIT, CRISC
Advisor – ISACA India Task Force

Objective of the Presentation

Securing “Sensitive Personal Data or Information”(SPDI) is now mandated by India’s Information Technology (Amendment) Act, 2008. The presentation will provide an approach to achieve this objective using the COBIT 5 framework.

Sensitive personal data or information is PI relating to:

i. Password
ii. Financial information such as Bank account or credit card or debit card or other payment instrument details
iii Physical, physiological and mental health condition
iv. Sexual orientation
v. Medical records and history
vi. Biometric information

Information that is freely available/ in public domain or under RTI Act, 2005 or other law not regarded as SPDI

Who is obliged to protect sensitive personal data?

Every entity (body corporate) that:

- Possesses, deals with or handles <u>any sensitive personal data</u> or information
- <u>In a computer resource</u> which it owns, controls or operates

“Body corporate” means any company and includes:

- A firm (such as a partnership firm)
- Sole proprietorship (such as a consultancy firm owned by a single person)
- Other association of individuals (such as professional bodies and organizations) <u>engaged in commercial or professional activities.</u>

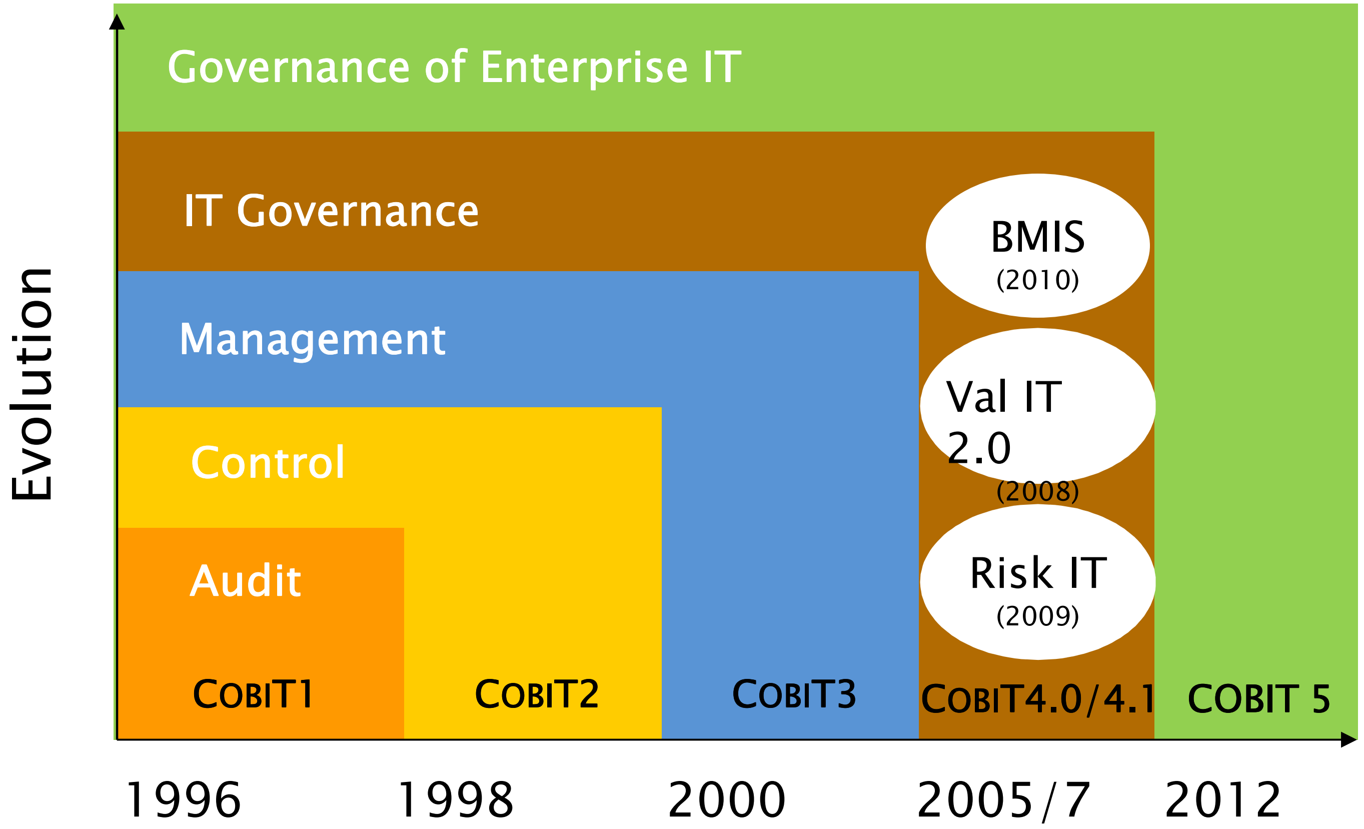
Effect of SPDI breach

- Negligence in implementing/maintaining Reasonable Security Practices & Procedures [RSPP] , causing wrongful loss/gain could lead to damages [compensation] to person affected
- RSPP should secure against unauthorized access/damage/change/impairment/use/ disclosure – in breach/violation of law, contract or GOI prescribed RSPP

Penalty for intentional breach Section 72 A

- Any person [including intermediary] providing services under lawful contract, who discloses PI with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, without consent/in breach of contract,
- Imprisonment for up to three years, or fine up to Rs. 5 lakh [Rupees 0.5 million] or both

The Evolution of COBIT 5



COBIT 5 Principles

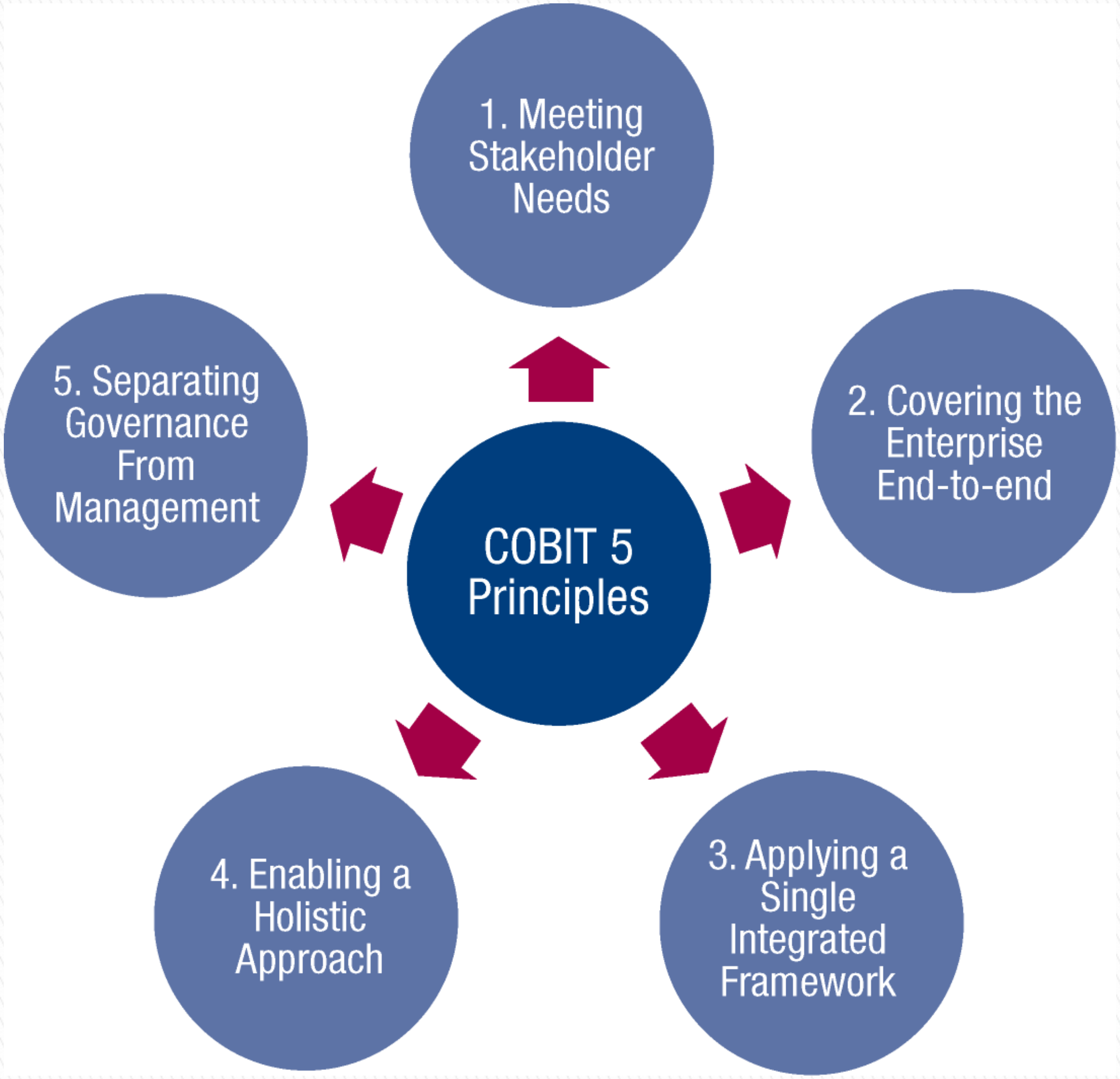

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
COBIT 5 Principles
5. Separating Governance From Management
4. Enabling a Holistic Approach
3. Applying a Single Integrated Framework

Figure 1 – COBIT 5 Principles

COBIT 5 Goals Cascade

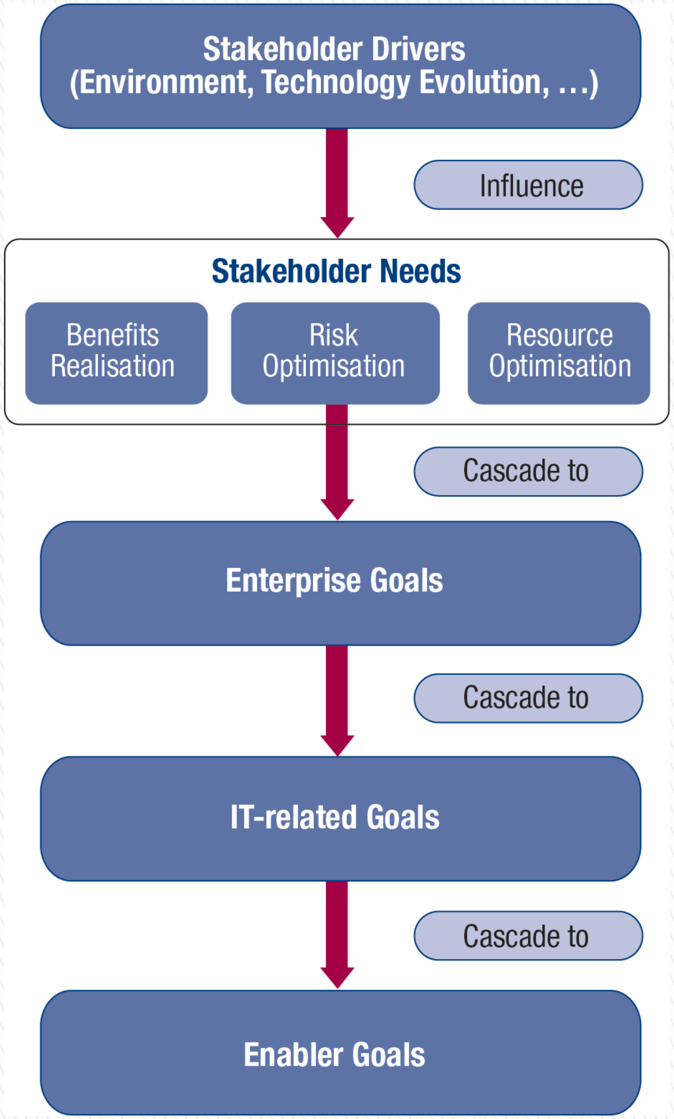


Figure 2 – COBIT 5 Goals Cascade Overview

The External & Internal Stakeholders

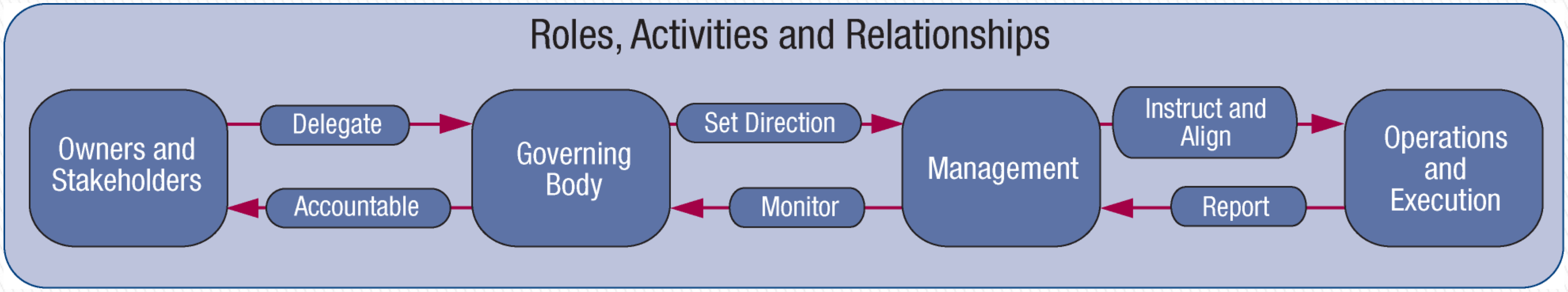


Figure 3 – Key Roles, Activities and Relationships

COBIT 5 Enterprise Enablers

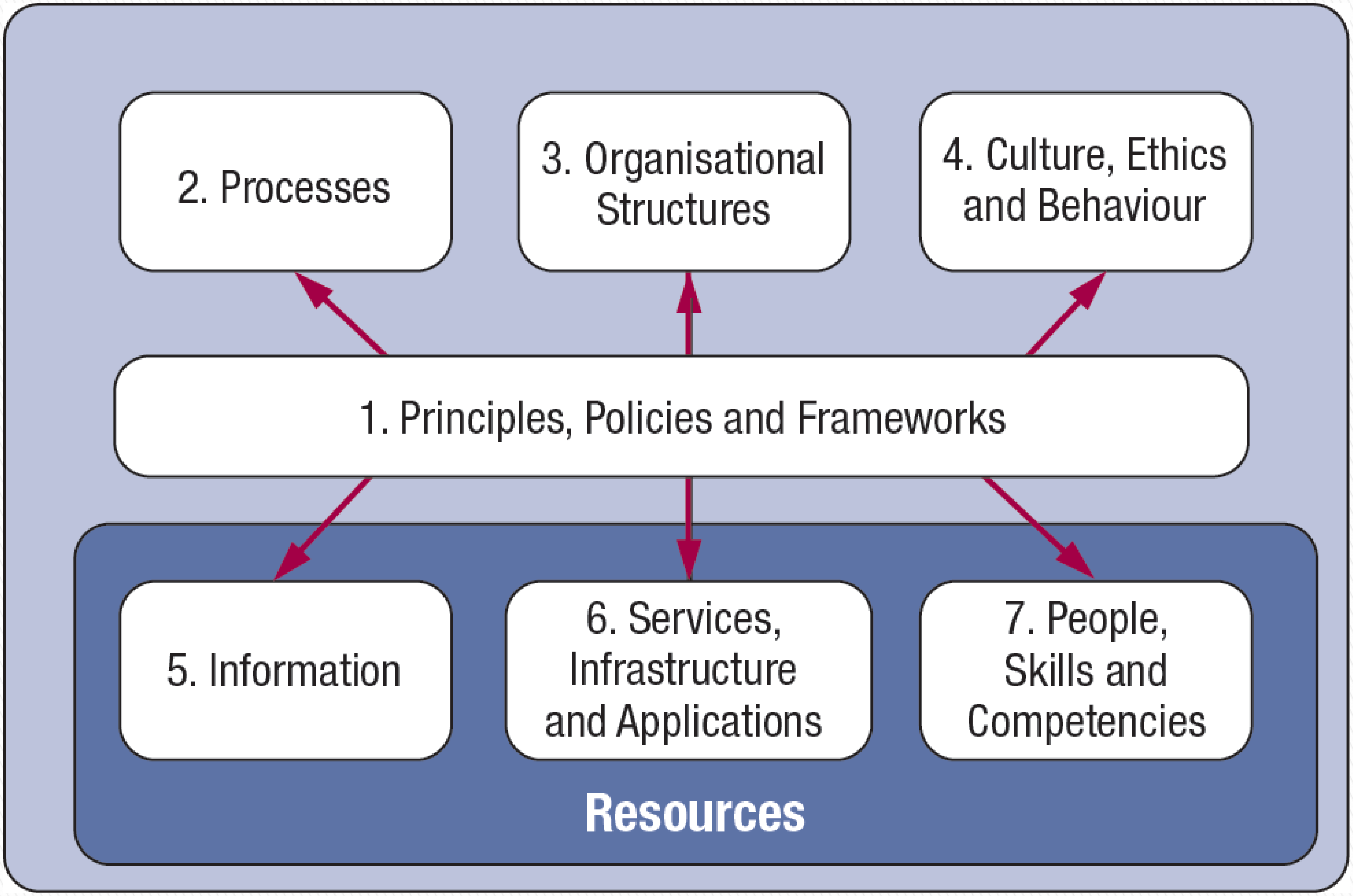
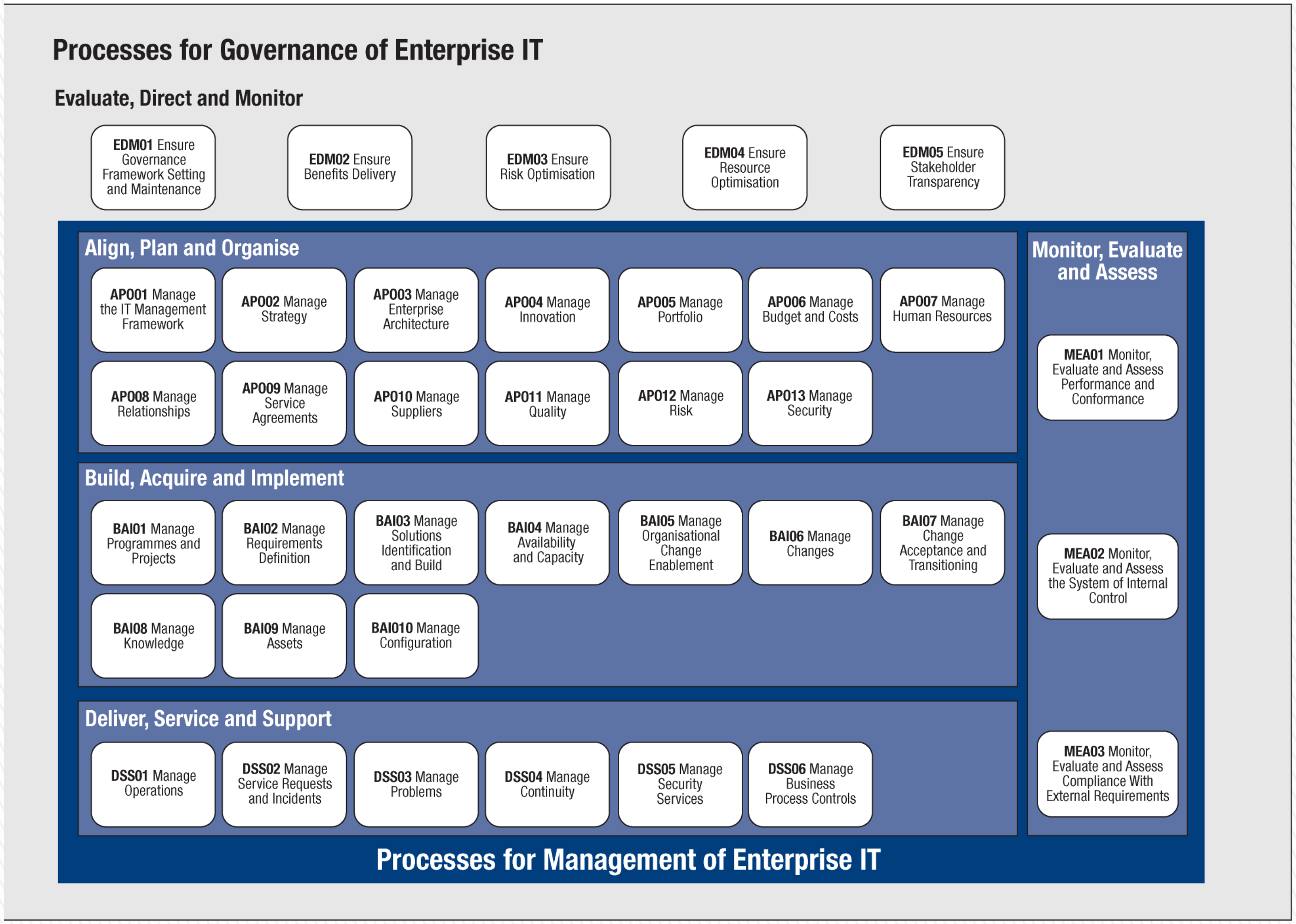

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Figure 8 – COBIT 5 Enterprise Enablers

Enabler 1: Policies and procedures required for securing SPDI

1. Privacy policy for SPDI
2. Procedures for the privacy policy for SPDI
3. SPDI security policies
4. SPDI security procedures

Enabler 2: Processes



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- **EDM01** Ensure Governance Framework Setting and Maintenance
- **EDM02** Ensure Benefits Delivery
- **EDM03** Ensure Risk Optimisation
- **EDM04** Ensure Resource Optimisation
- **EDM05** Ensure Stakeholder Transparency

Align, Plan and Organise

- **APO01** Manage the IT Management Framework
- **APO02** Manage Strategy
- **APO03** Manage Enterprise Architecture
- **APO04** Manage Innovation
- **APO05** Manage Portfolio
- **APO06** Manage Budget and Costs
- **APO07** Manage Human Resources
- **APO08** Manage Relationships
- **APO09** Manage Service Agreements
- **APO10** Manage Suppliers
- **APO11** Manage Quality
- **APO12** Manage Risk
- **APO13** Manage Security

Build, Acquire and Implement

- **BAI01** Manage Programmes and Projects
- **BAI02** Manage Requirements Definition
- **BAI03** Manage Solutions Identification and Build
- **BAI04** Manage Availability and Capacity
- **BAI05** Manage Organisational Change Enablement
- **BAI06** Manage Changes
- **BAI07** Manage Change Acceptance and Transitioning
- **BAI08** Manage Knowledge
- **BAI09** Manage Assets
- **BAI010** Manage Configuration

Deliver, Service and Support

- **DSS01** Manage Operations
- **DSS02** Manage Service Requests and Incidents
- **DSS03** Manage Problems
- **DSS04** Manage Continuity
- **DSS05** Manage Security Services
- **DSS06** Manage Business Process Controls

Monitor, Evaluate and Assess

- **MEA01** Monitor, Evaluate and Assess Performance and Conformance
- **MEA02** Monitor, Evaluate and Assess the System of Internal Control
- **MEA03** Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Figure 9 – COBIT 5 Process Reference Model

Enabler 3: Organisation Structure

- Governing Body – Board, CEO
- Management Committee – CEO, CFO, CIO, CISO, and all the 'C' level executives of the organization
- Operation and Execution Team – Business process owners, Human resource manager, Security officer, Internal auditors, Privacy officer, IT users, etc.

Enabler 4: Culture, Ethics and Behaviour

- Behaviour
  - Organisational level
  - Individual level

- Leadership
  - Influencing behaviour through communication, enforcement, rules and norms
  - Influencing behaviour through incentives and rewards

Enabler 5: Information

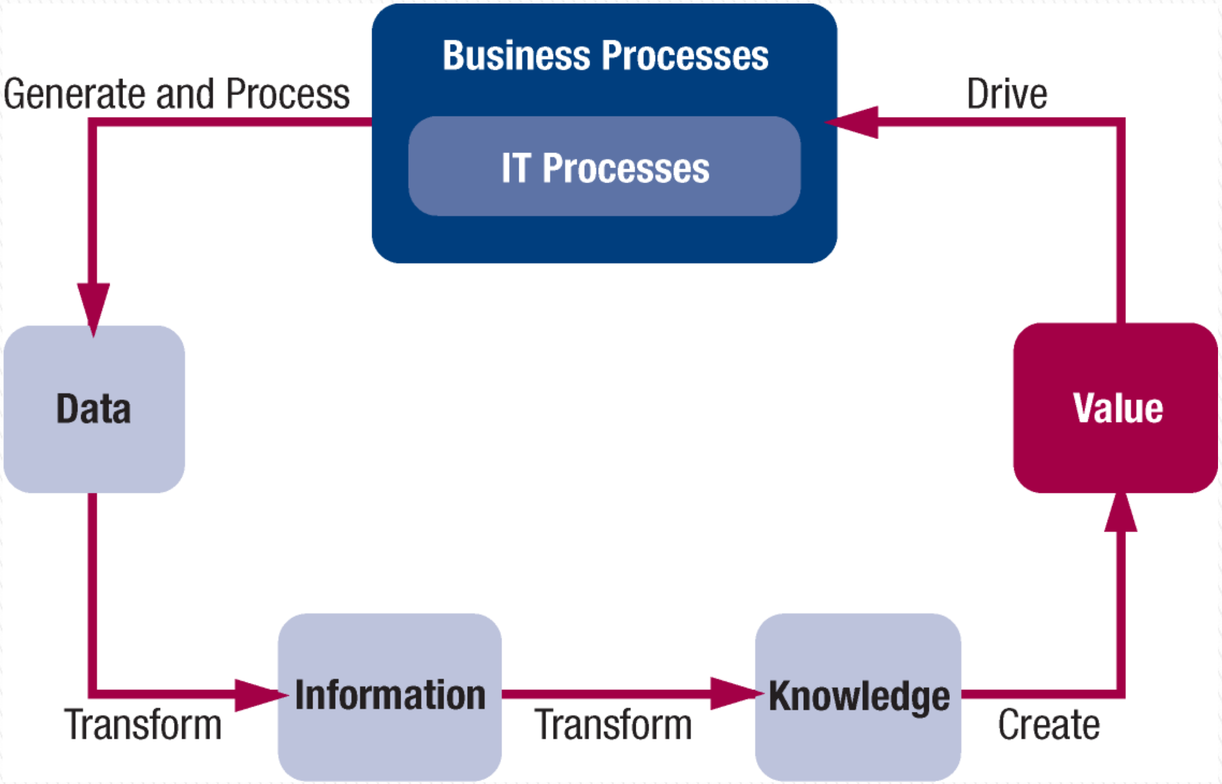


Figure 11 – COBIT Metadata Information Cycle

Enabler 6: Services, Infrastructure and Applications

- Create service capabilities to meet the SPDI security requirements
- Emphasis on security of SPDI in the service architectural design
- Applications designed with focus on security
- Service level agreements clearing defining the responsibility of service provide
- Confidentiality agreements with service providers

Enabler 7: People, Skills and Competencies

Make sure that the training is imparted at each level in the organisation

- Board and Chairman
- Management
- Operation and the Execution team
- General staff

Learn More!

This presentation is a brief summary of the publication:

Securing Sensitive Personal Data or Information:Using COBIT 5 for India's IT Act

Available now! Visit www.isaca.org/topic-India to join the discussion group and download the material.

Questions?

Trust in, and value from, information systems

Thank you!
Avinash W. Kadam
awkadam@isaca.org