CS4050 – WEEK 6: INFORMATION SYSTEMS AUDIT AND CONTROL

FAST NUCES – SPRING 2024

BS COMPUTER SCIENCE

CHAPTER 2: GOVERNANCE & MANAGEMENT OF IT

- Part A: IT Governance
  - IT Governance & IT Strategy
  - IT Related Frameworks
  - IT Standards, Policies & Procedures
  - Organizational Structure
  - Enterprise Architecture
  - Enterprise Risk Management
  - Maturity Models
  - Laws, Regulations & Industry Standards

- Part B: IT Management
  - IT Resource Management
  - IT Service Provider Acquisition & Management
  - IT Performance Monitoring & Reporting
  - Quality Assurance & Quality Management of IT
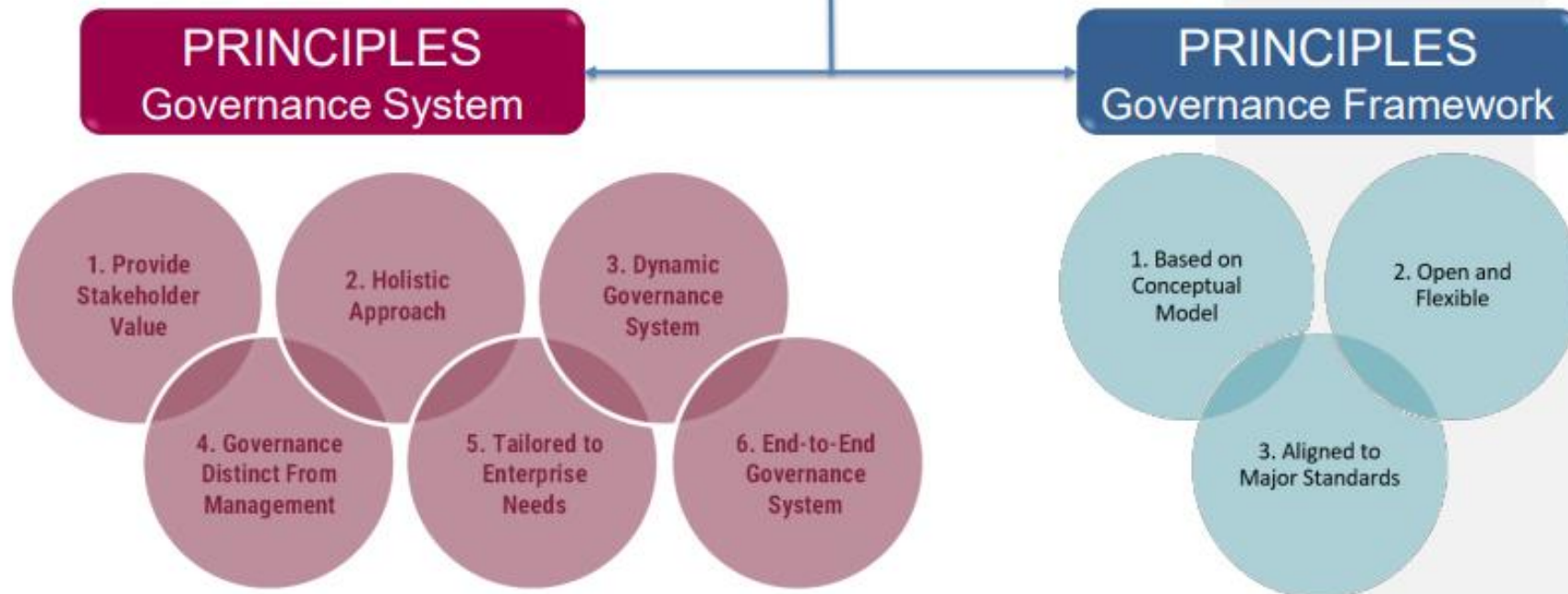
PART A: IT GOVERNANCE

- IT Governance and IT Strategy

  - Corporate Governance

  - Enterprise Governance of Information Technology (EGIT)

  - Governance VS Management

  - Information Security Governance

  - Information Systems/Technology Strategy

  - IT Related Frameworks

    (i) COBIT (ii) ITIL (iii) ISO 27000 (iv) O-ISM3 (v) ISO 38500:2015 (vi) ISO 20000 (vii) ISO 3100

KEY CONCEPTS
GOVERNANCE AND MANAGEMENT OBJECTIVES

Similar to COBIT 5, The governance and management objectives in COBIT® 2019 are grouped into five domains. The domains have names that express the key purpose and areas of activity of the objectives contained in them.

Governance objectives	Management objectives			
EDM Evaluate, Direct and Monitor	**APO** Align, Plan and Organize	**BAI** Build, Acquire and Implement	**DSS** Deliver, Service and Support	**MEA** Monitor, Evaluate and Assess

COBIT 2019

EDM01—Ensured Governance Framework Setting and Maintenance	EDM02—Ensured Benefits Delivery	EDM03—Ensured Risk Optimization	EDM04—Ensured Resource Optimization	EDM05—Ensured Stakeholder Engagement

APO01—Managed I&T Management Framework	APO02—Managed Strategy	APO03—Managed Enterprise Architecture	APO04—Managed Innovation	APO05—Managed Portfolio	APO06—Managed Budget and Costs	APO07—Managed Human Resources
APO08—Managed Relationships	APO09—Managed Service Agreements	APO10—Managed Vendors	APO11—Managed Quality	APO12—Managed Risk	APO13—Managed Security	APO014—Managed Data

MEA01—Managed Performance and Conformance Monitoring

BAI01—Managed Programs	BAI02—Managed Requirements Definition	BAI03—Managed Solutions Identification and Build	BAI04—Managed Availability and Capacity	BAI05—Managed Organizational Change	BAI06—Managed IT Changes	BAI07—Managed IT Change Acceptance and Transitioning
BAI08—Managed Knowledge	BAI09—Managed Assets	BAI10—Managed Configuration	BAI11—Managed Projects			

MEA02—Managed System of Internal Control

MEA03—Managed Compliance With External Requirements

DSS01—Managed Operations	DSS02—Managed Service Requests and Incidents	DSS03—Managed Problems	DSS04—Managed Continuity	DSS05—Managed Security Services	DSS06—Managed Business Process Controls

MEA04—Managed Assurance

Known as the Process Reference Model, or PRM in COBIT 5, COBIT® 2019 identifies this as the **COBIT Core Model**.

IT STRATEGY – WHAT IT SHOULD ACHIEVE?

Anoof- IT Strategy Report

- Alignment of IT with the business direction
- Relevance of developments in IT from a business perspective
- The achievement of strategic IT objectives
- Availability of suitable IT resources, skills and infrastructure to meet the strategic objectives
- Optimization of IT costs, including the role and value delivery of external IT sourcing
- Risk, return and competitive aspects of IT investments
- Progress of major IT projects
- The contribution of IT to the business
- Exposure to IT risk, including compliance risk and setting direction on how to contain it
- Direction to management relative to IT strategy

IMPORTANCE OF IT STEERING COMMITTEE

ROLE OF IT STEERING COMMITTEE

❖ Providing input on the growth or development of a business or initiative.

❖ Addressing concerns and offering guidance on budgeting, marketing, recruiting, and other financial issues.

❖ Identifying the outcomes or objectives that the project must achieve.

❖ Prioritize the steps and objectives that must be completed to meet the project's objectives.

❖ Assisting in the formulation of business-related policies, processes, and guidelines.

❖ Identifying, monitoring, and eliminating potential operational risks.

❖ Setting project deadlines or timelines and keeping track of progress.

❖ Monitoring the final work's quality.

❖ Making plans for how a client or consumer will react to a product or service.

❖ Analyzing and discussing changes that have occurred or will occur to guarantee the project's success.

❖ In the workplace, encouraging team members to collaborate.

❖ Where relevant, providing further insights on business or project concerns.
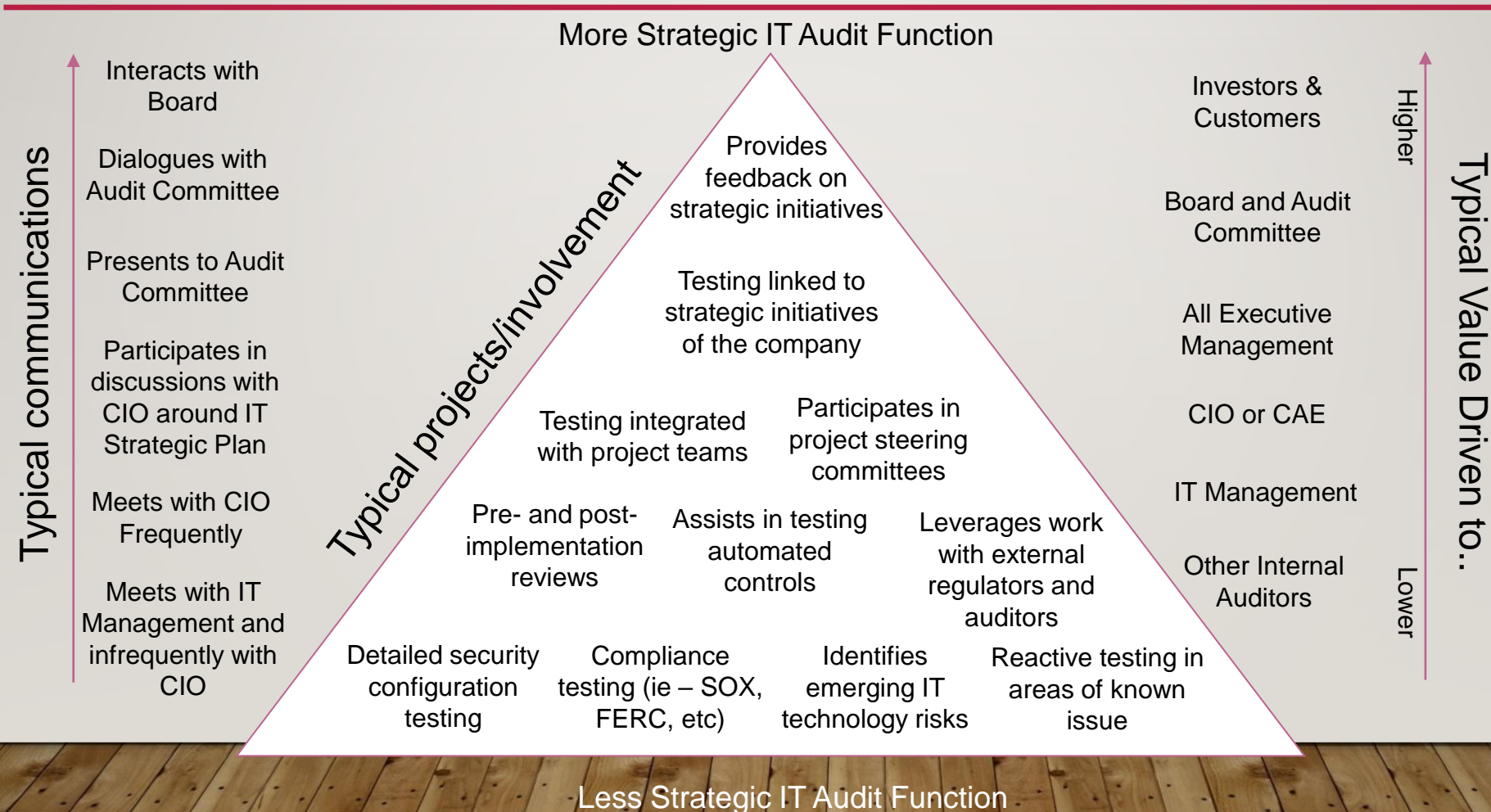
SEGREGATION OF DUTIES

	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database	Network	Systems	Security Administrator	SystemsProgrammer	Quality Assurance
Control Group		X	X	X		X	X	X	X	X		X	
Systems Analyst	X			X	X		X				X		X
Application Programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X	X	X		X	X		X	
Network Administrator	X		X	X	X	X	X	X					
System Administrator	X		X	X		X	X	X				X	
Security Administrator		X	X			X	X					X	
Systems Programmer	X		X	X	X	X	X	X		X	X		X
Quality Assurance		X	X		X							X	

X—Combination of these functions may create a potential control weakness.

ROLES VS. ACTIVITIES

	DBA Staging	DBA Production	System Administrator Staging	System Administrator Production	Manager	Programmer	Security Officer	User
Uses Application	X	X	X	X	X	X	X	
Receives Updates—Database		X				X		
Receives Updates—Application				X		X		
Initiates Change								
Authorizes Change	X	X	X	X		X		
Tests Updates—Database		X	X	X	X	X	X	X
Tests Updates—Application	X	X		X	X	X	X	X
Implements Updates—Database	X		X	X	X	X	X	X
Implements Updates—Application	X	X	X			X	X	X
Access to Source Code		X		X			X	X
Administrative Access—Database O/S-Staging		X	X	X	X	X		X
Administrative Access—Database O/S-Production	X		X	X	X	X		X
Administrative Access—Application O/S-Staging	X	X		X	X	X		X
Administrative Access—Application O/S-Production	X	X	X		X	X		X
Administrative Access—Staging Database		X	X	X	X			X
Administrative Access—Staging Application	X	X		X	X			X
Administrative Access—Production Database	X		X	X	X	X		X
Administrative Access—Production Application	X	X	X		X	X		X
Monitors Changes and Security Events—Database	X-if not also monitored by the security officer	X- if not also monitored by the security officer						X
Monitors Changes and Security Events—Application			X-if not also monitored by the security officer	X-if not also monitored by the security officer				X

QUALITIES FOUND IN SUCCESSFUL IT AUDIT FUNCTIONS

More Strategic IT Audit Function

Typical communications
- Interacts with Board
- Dialogues with Audit Committee
- Presents to Audit Committee
- Participates in discussions with CIO around IT Strategic Plan
- Meets with CIO Frequently
- Meets with IT Management and infrequently with CIO

Typical projects/involvement
- Provides feedback on strategic initiatives
- Testing linked to strategic initiatives of the company
- Testing integrated with project teams
- Participates in project steering committees
- Pre- and post-implementation reviews
- Assists in testing automated controls
- Leverages work with external regulators and auditors
- Detailed security configuration testing
- Compliance testing (ie – SOX, FERC, etc)
- Identifies emerging IT technology risks
- Reactive testing in areas of known issue

Typical Value Driven to.. (Higher / Lower)
- Investors & Customers
- Board and Audit Committee
- All Executive Management
- CIO or CAE
- IT Management
- Other Internal Auditors

Less Strategic IT Audit Function

RISK CONTROL MATRIX & IT GENERAL CONTROLS

RCM – IT General
Control

Quiz No. 1