CS4050 – WEEK 4: INFORMATION SYSTEMS AUDIT AND CONTROL

FAST NUCES – SPRING 2024

BS COMPUTER SCIENCE

DOMAIN 1: PART B – IS AUDITING PROCESS

- Audit Evidence Collection Techniques:
  - Reviewing IS organization structures
  - Reviewing IS policies and procedures
  - Reviewing IS standards
  - Reviewing IS documentation
  - Interviewing appropriate personnel
  - Observing processes and performance
  - Reperformance
  - Walk-throughs

CONCLUDING THE AUDIT PROCESS

- Evidence Collection Techniques
- Data Analytics
- Continuous Auditing and Monitoring
- Reporting & Communications Techniques
- Audit Report Structure and Content
- Audit Documentation
- Quality Assurance and Improvement of Audit Process
    - Control Self Assessment
- Integrated Auditing

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

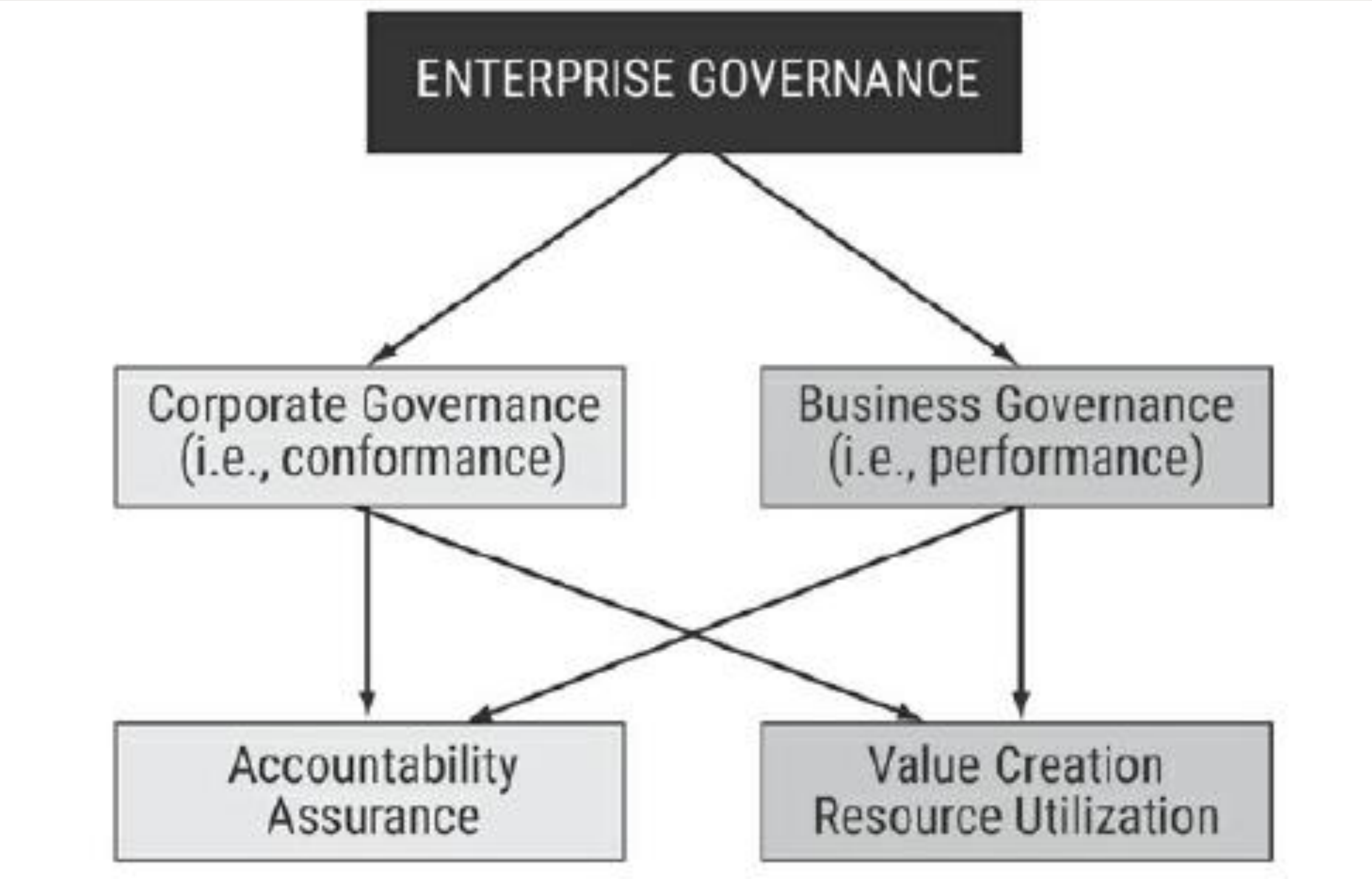
PART A: IT GOVERNANCE

- 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

SBP 2017 -
ETGRMF

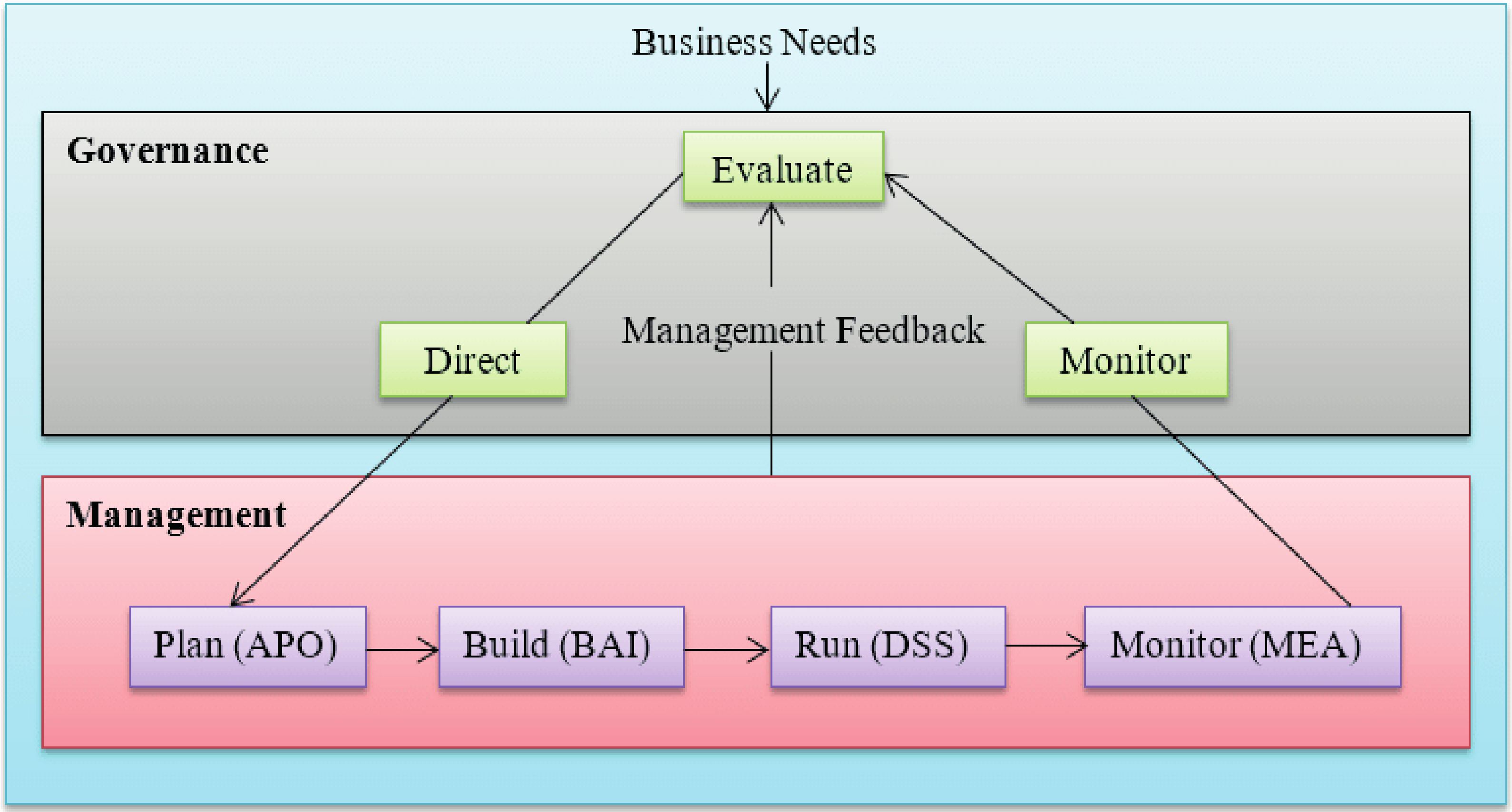
ENTERPRISE GOVERNANCE FRAMEWORK


ENTERPRISE GOVERNANCE
Corporate Governance (i.e., conformance)
Business Governance (i.e., performance)
Accountability Assurance
Value Creation Resource Utilization

GOVERNANCE VS. MANAGEMENT

Governance - Ensures that stakeholder needs, conditions & options are evaluated to determine balanced, agreed-on enterprise objectives; direction is set through prioritization & decision-making; also, performance and compliance are monitored against agreed-on direction and objectives

Management - Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives



OBJECTIVES OF EGIT

- Better return from IT investments
- Meeting increasing regulatory requirements
- Selection of service providers and management of service outsourcing
- Adoption of IT standards, control frameworks, policies, etc.
- Need to optimize costs
- Benchmarking of IT service quality

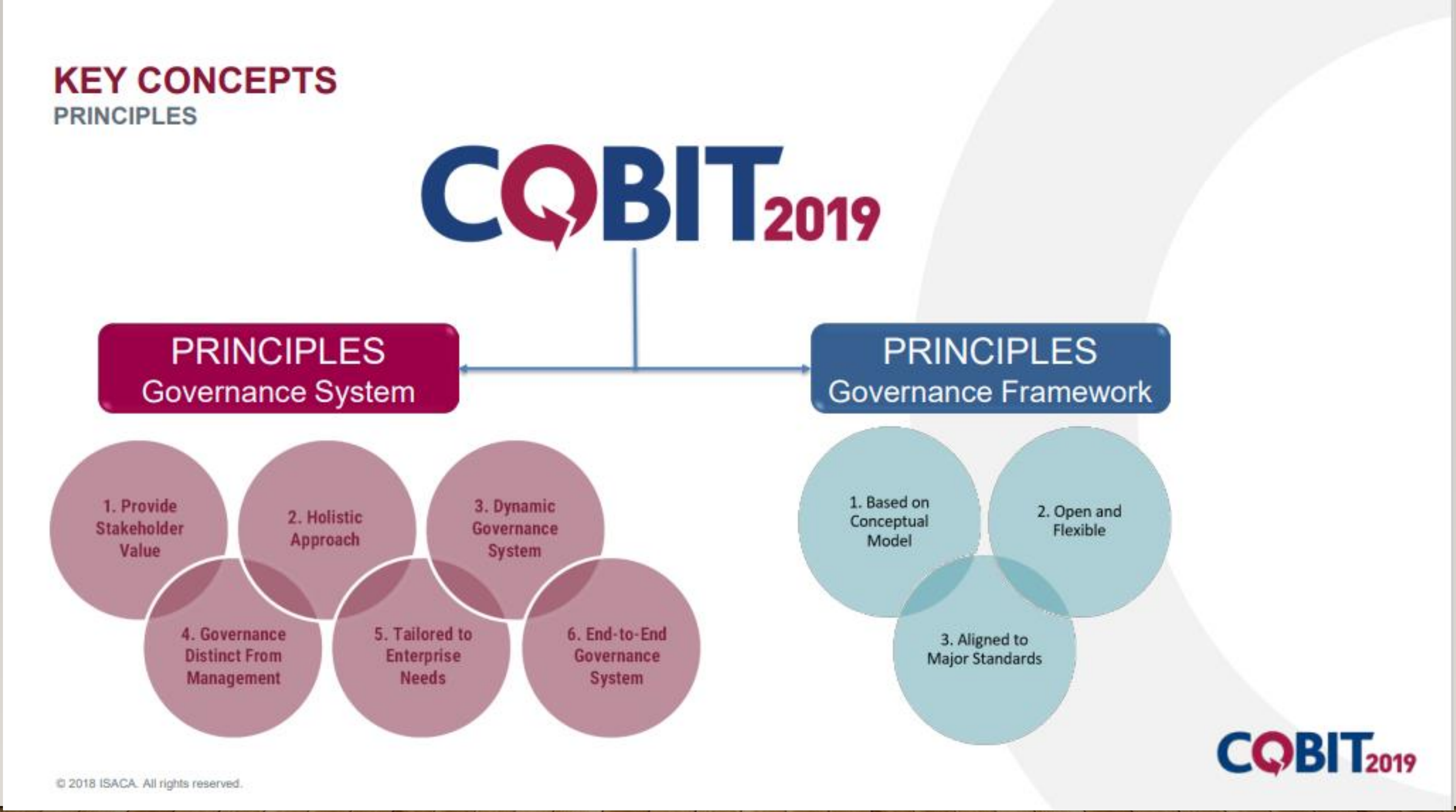
The IS auditor is expected to play effective role in giving assurance on EGIT

INFORMATION SECURITY GOVERNANCE

- A comprehensive security strategy intrinsically linked with business and IT objectives
- Governing security policies that address each aspect of strategy, controls and regulation
- A complete set of standards for each policy to ensure that procedures and guidelines comply with policy
- An effective security organizational structure void of conflicts of interest
- Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness

IT RELATED FRAMEWORKS

- Control Objectives for Information & Related Technology (COBIT)
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000
- The Information Technology Infrastructure Library (ITIL®)
- The Open Information Security Management Maturity Model (OISM3)
- ISO/IEC 38500:2015: Information technology—Governance of IT for the organization
- ISO/IEC 20000
- ISO 3100:2018: Risk management—Guidelines



KEY CONCEPTS

PRINCIPLES

COBIT 2019

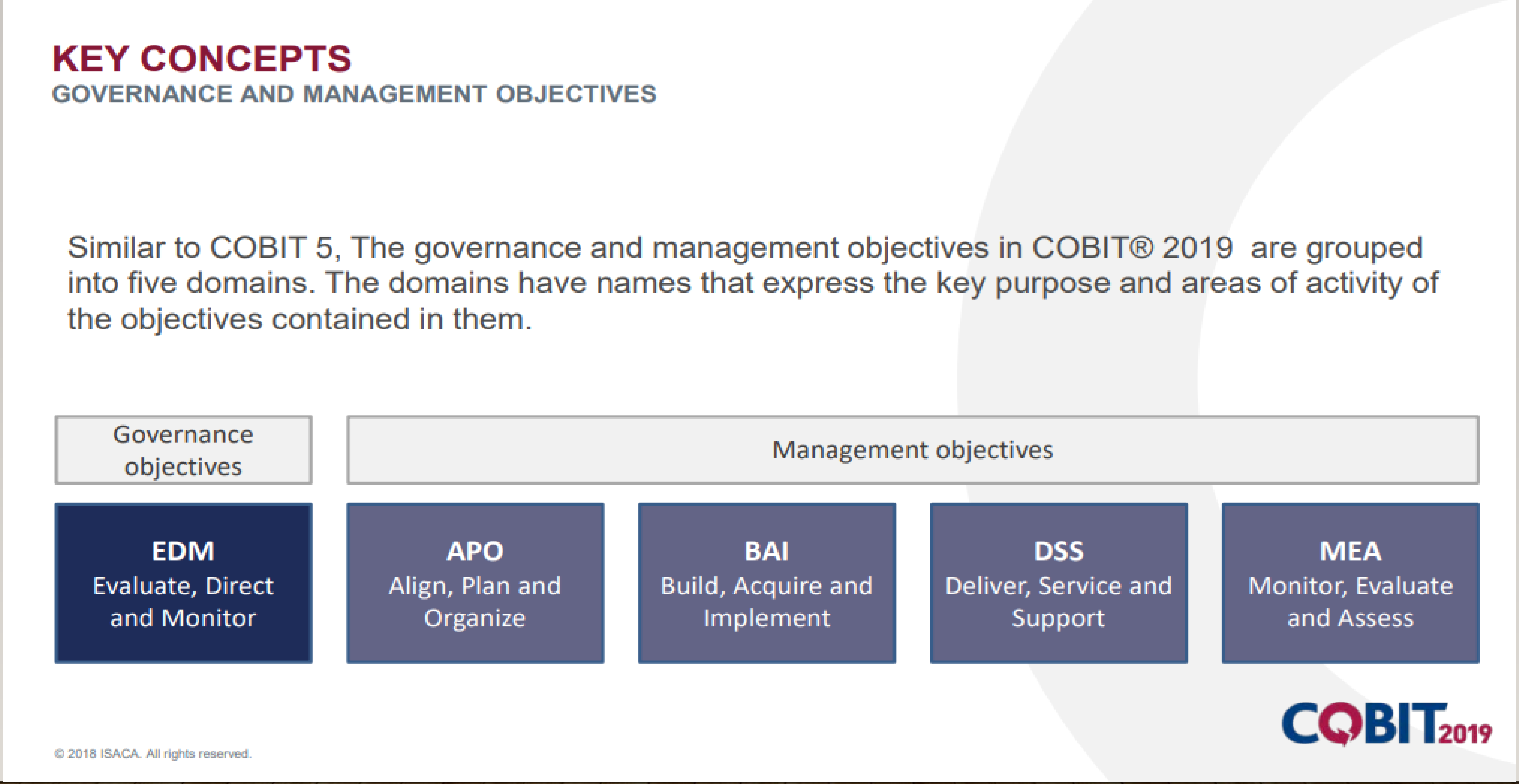
PRINCIPLES
Governance System

1. Provide Stakeholder Value
2. Holistic Approach
3. Dynamic Governance System
4. Governance Distinct From Management
5. Tailored to Enterprise Needs
6. End-to-End Governance System

PRINCIPLES
Governance Framework

1. Based on Conceptual Model
2. Open and Flexible
3. Aligned to Major Standards

COBIT 2019

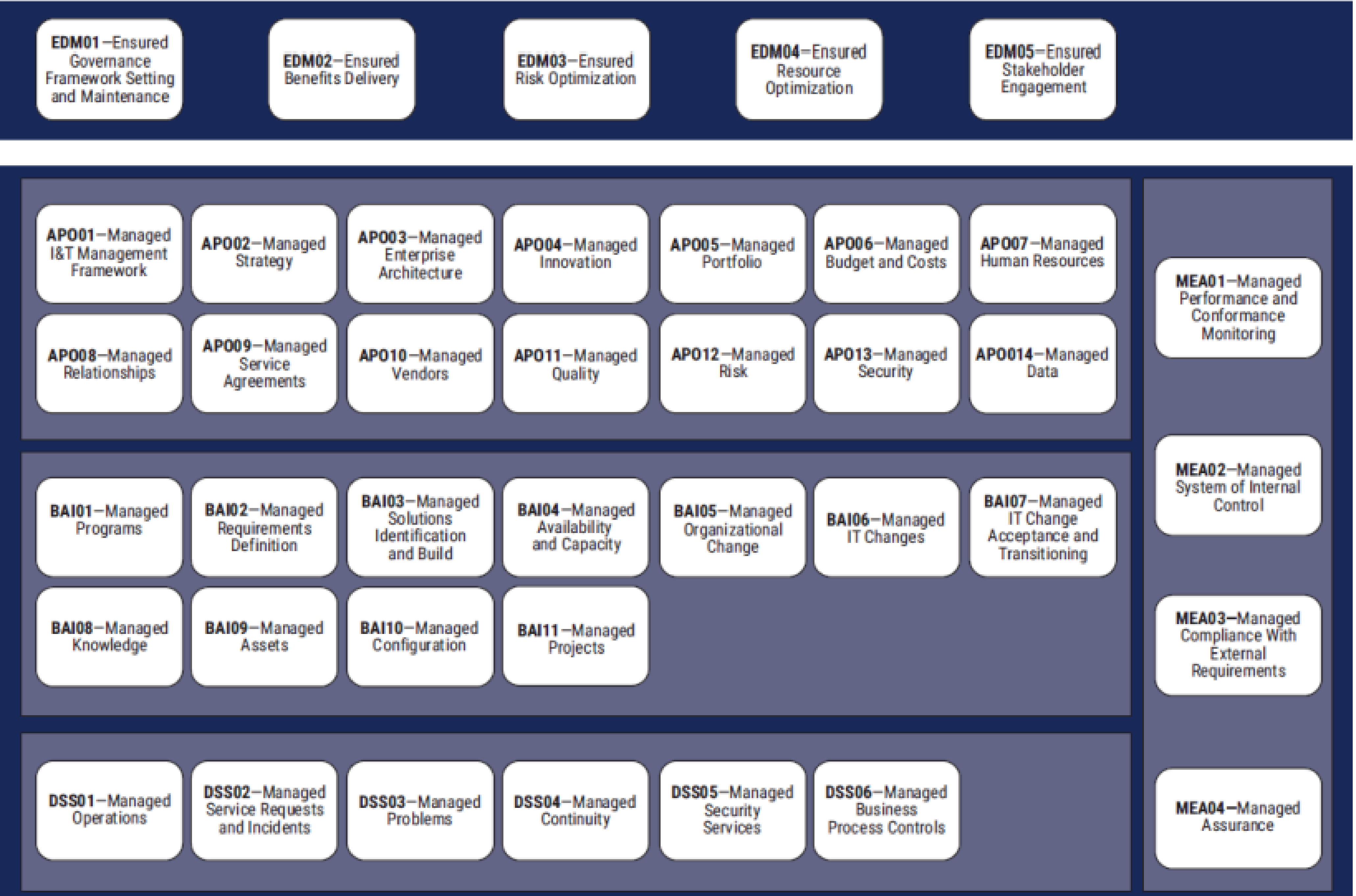


KEY CONCEPTS

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



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

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

DSS01—Managed Operations

DSS02—Managed Service Requests and Incidents

DSS03—Managed Problems

DSS04—Managed Continuity

DSS05—Managed Security Services

DSS06—Managed Business Process Controls

MEA01—Managed Performance and Conformance Monitoring

MEA02—Managed System of Internal Control

MEA03—Managed Compliance With External Requirements

MEA04—Managed Assurance

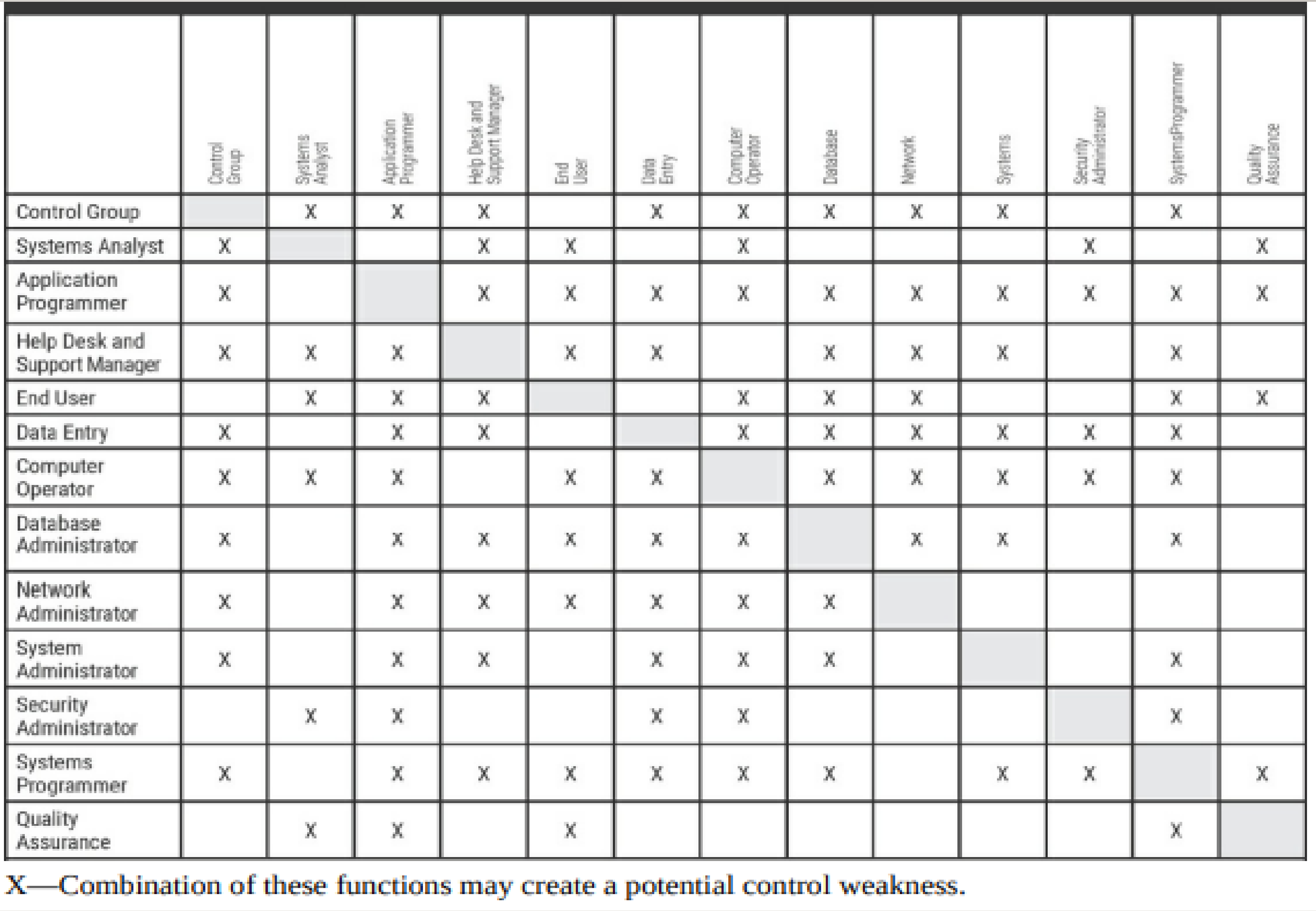
Reference: COBIT® 2019 Framework: Introduction and Methodology, Chapter 4 Basic Concepts: Governance Systems and Components, Figure 4.2

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?

- Alignment of IT with the business direction
- 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

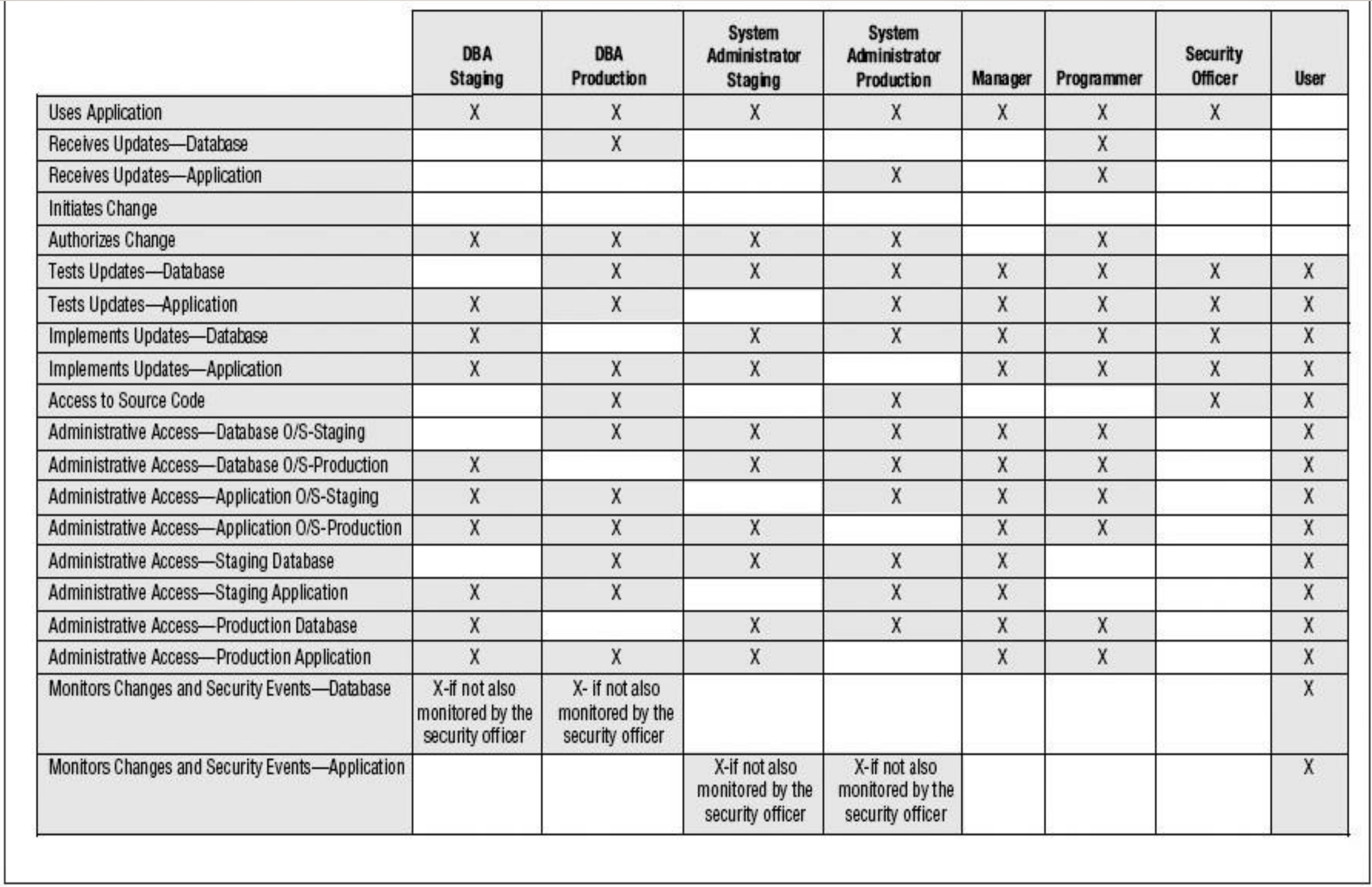
SEGREGATION OF DUTIES



	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	

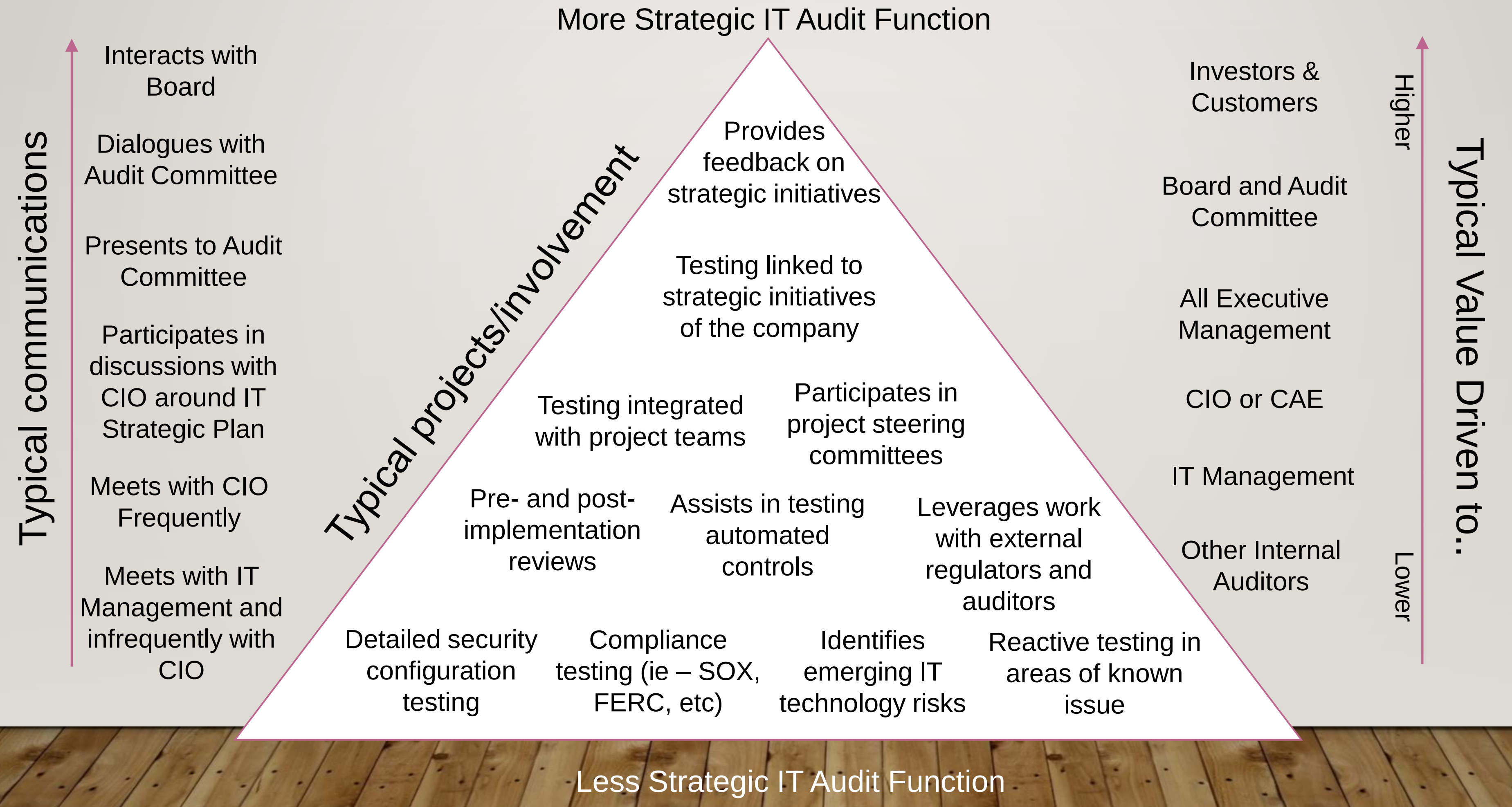
X—Combination of these functions may create a potential control weakness.

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	X
Access to Source Code		X		X			X	X
Administrative Access—Database 0/S-Staging		X	X	X	X	X		X
Administrative Access—Database 0/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

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

Less Strategic IT Audit Function

Typical projects/involvement

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 Value Driven to..

Higher

Investors & Customers

Board and Audit Committee

All Executive Management

CIO or CAE

IT Management

Other Internal Auditors

Lower