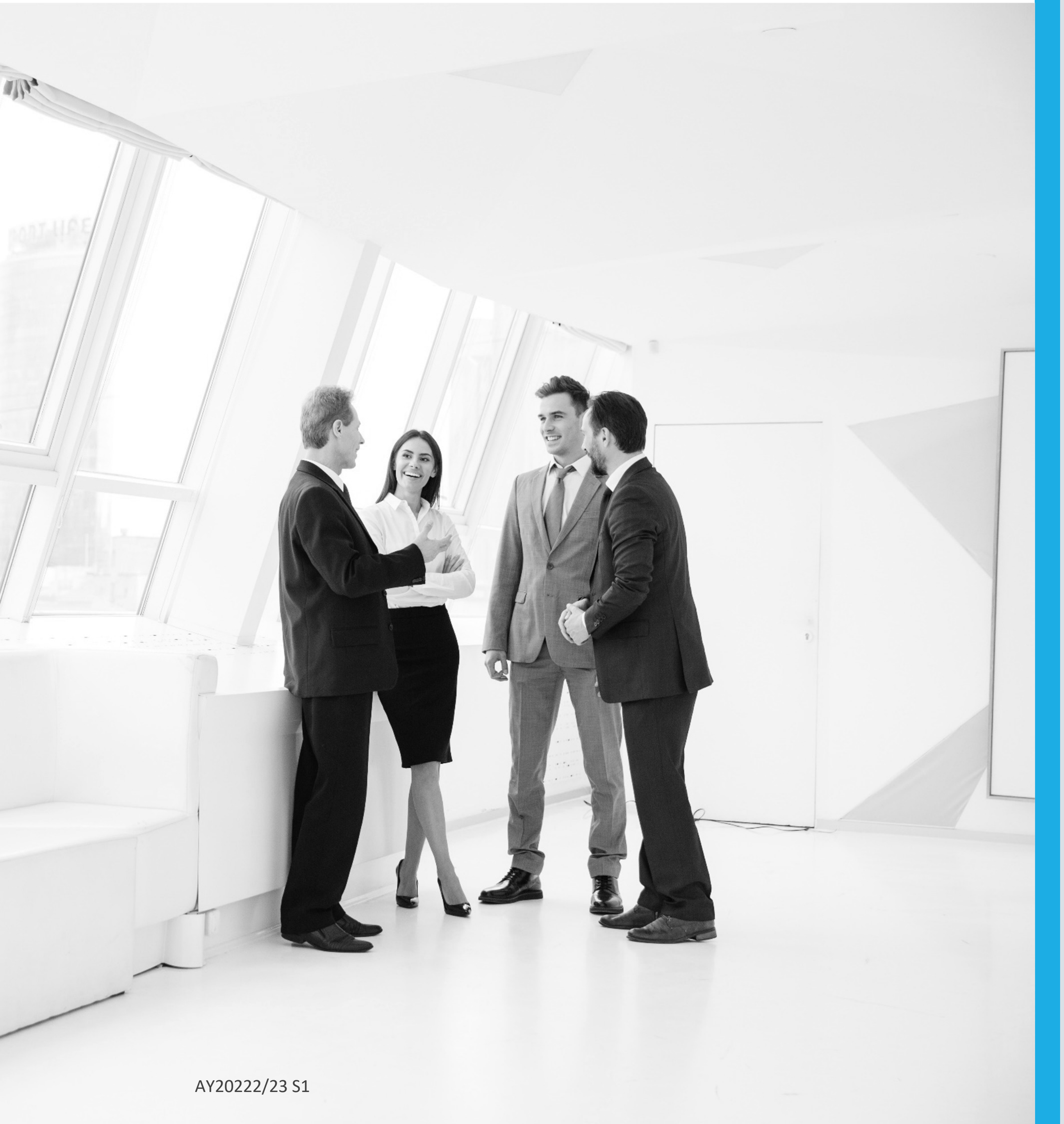
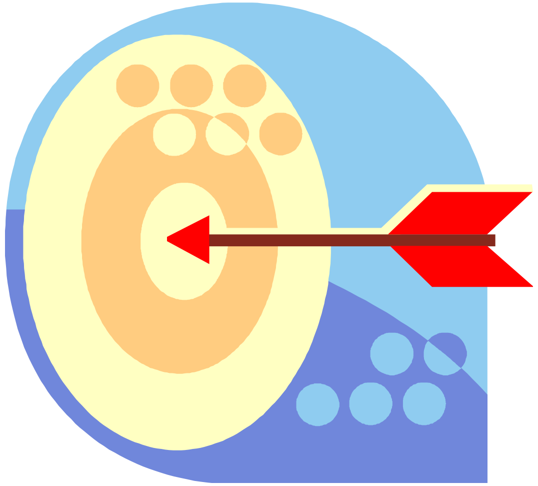


Governance, Risk & Compliance

TOPIC 2 : FRAMEWORK FOR GOVERNANCE OF ENTERPRISE IT

Objectives

- Enterprise Governance
- GEIT Frameworks
- Business Drivers for GEIT
- GEIT Enablers



Players

Board of Directors

Sets the overall direction of the company.

Accountable to the shareholders

Meets regularly to deliberate company matters.

CEO & Executive Management

Includes CEO and his immediate subordinates such as CFO, CIO, COO, etc

Executes the operational tasks of the organization based on direction set by the board

Employees

Do the actual work as set out by CEO & Executive Management

Responsible for the work done to CEO & Executive Management

Enterprise Governance

- High-profile cases of corporate failure and fraud has brought enterprise governance to business and political agendas.
  - What is the link between enterprise governance & politics?
- Several codes of conduct and frameworks for enterprise governance have been published to further the cause for enterprise governance.

Enterprise Governance

- Definition of enterprise governance by ISACA:
  - Enterprise governance is a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

Conformance & Performance

- In October 2003, the International Federation of Accountants published a report, which identifies two dimensions of enterprise governance :
  - Conformance
    - Addresses corporate structure, roles and executive remuneration.
  - Performance
    - Focus on strategy and value creation.
    - Enhance efficiency through managing of risk appetite.

Conformance & Performance

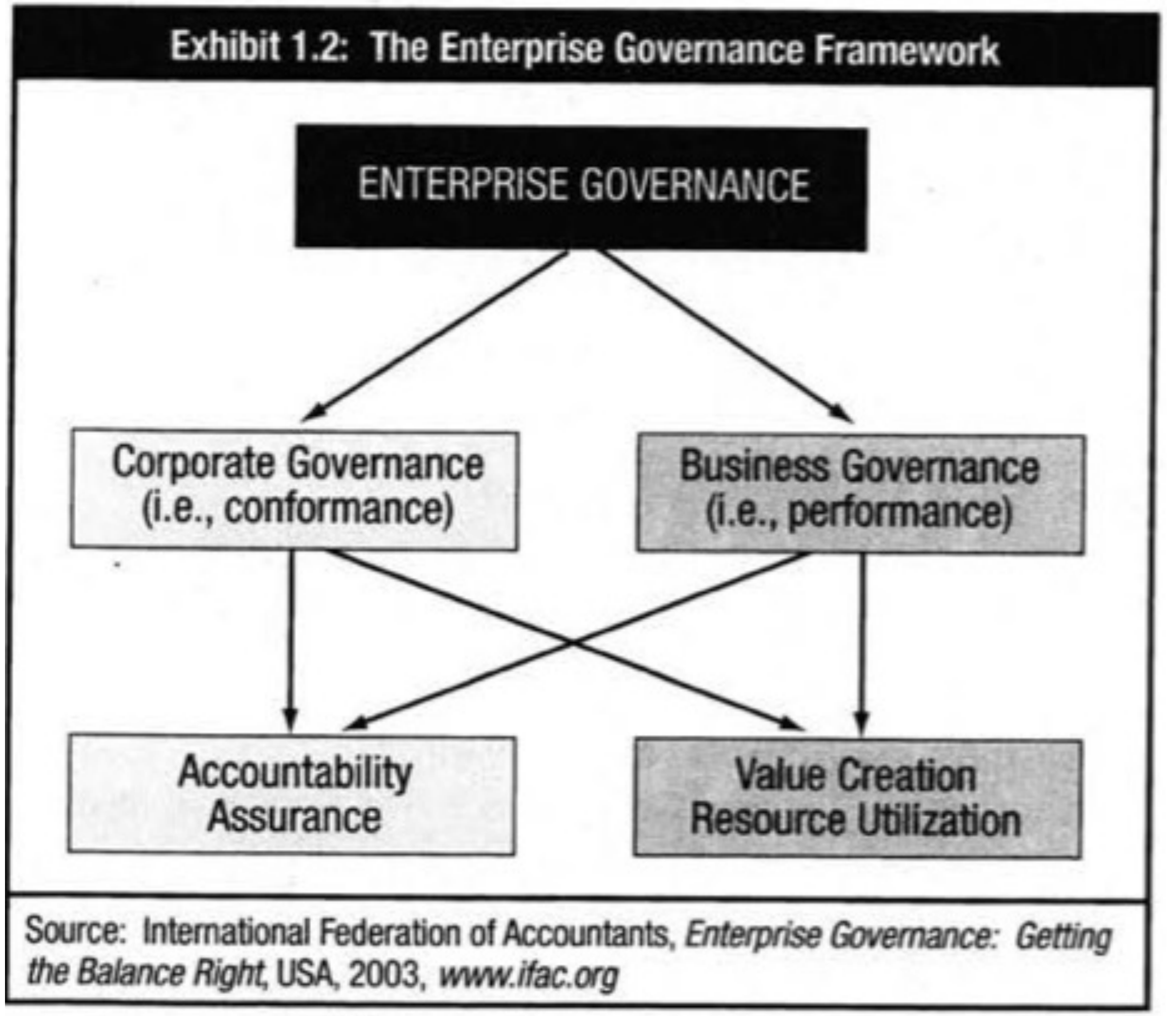


Exhibit 1.2: The Enterprise Governance Framework

ENTERPRISE GOVERNANCE

Corporate Governance (i.e., conformance)

Business Governance (i.e., performance)

Accountability Assurance

Value Creation Resource Utilization

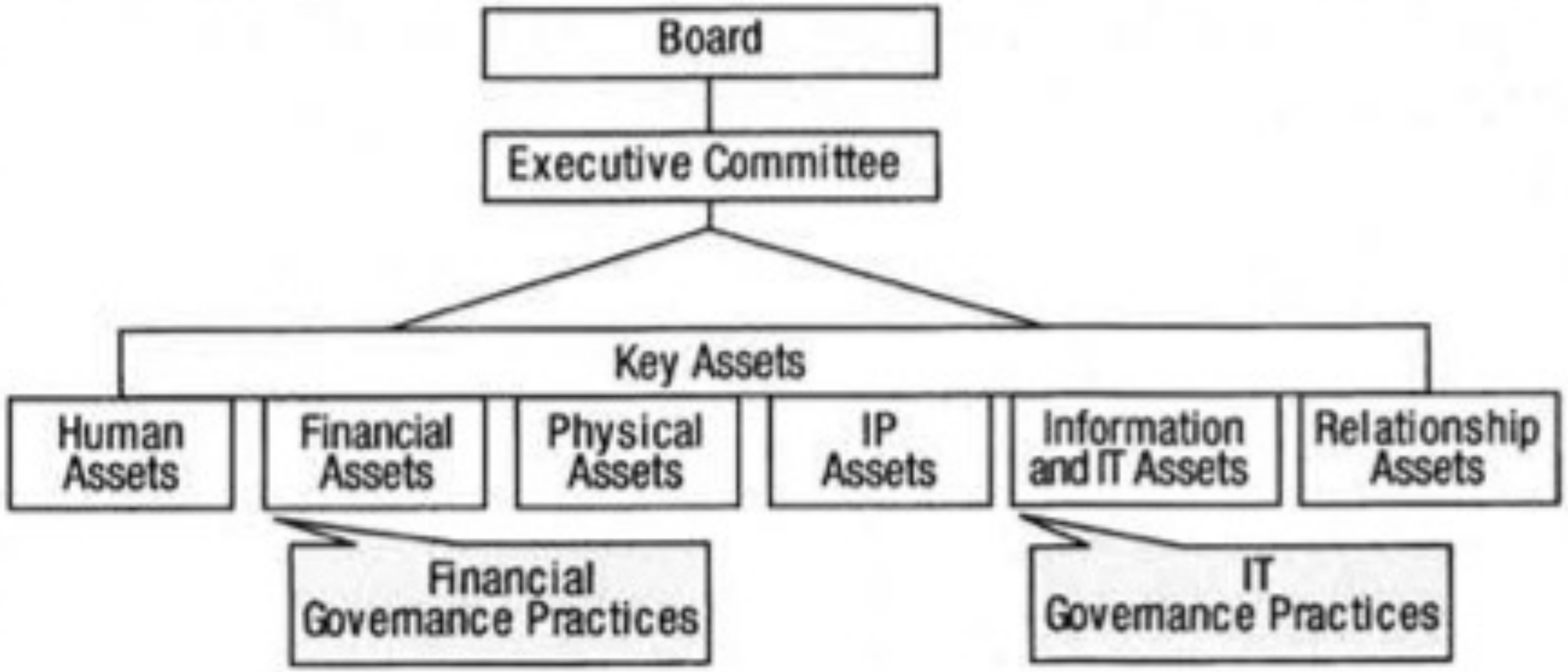
Source: International Federation of Accountants, *Enterprise Governance: Getting the Balance Right*, USA, 2003, *www.ifac.org*

Key Assets

- Enterprise governance comprise of six key assets that need to be governed :
  - Human assets
  - Financial assets
  - Physical assets
  - IP assets
  - Information & IT assets
  - Relationship assets

from Weill, Peter; Jeanne Ross: IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, USA, 2004.

Key Assets



Source: Weill, Peter; Jeanne Ross; *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, USA, 2004

GEIT Frameworks

- Many frameworks for the governance of enterprise IT have been published.
- They form best-practices which can be used to guide the management in implementing IT governance processes.
- They include those that target the
  - Governance of Enterprise IT
  - Management of Enterprise IT

GEIT Frameworks

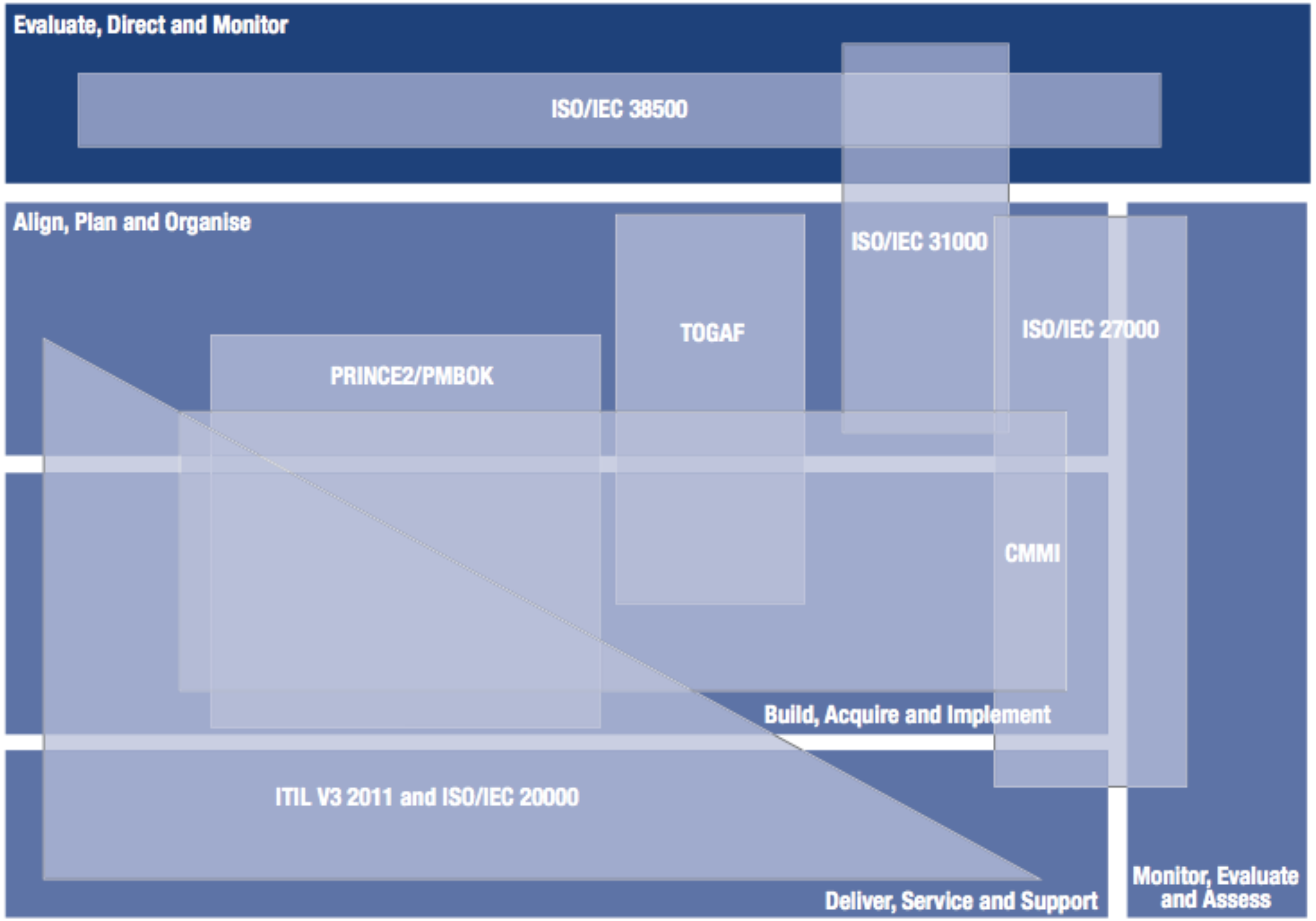
- Governance of enterprise IT
  - ISACA's COBIT
  - ISO 38500
- Management of enterprise IT
  - CMMI – Capability Maturity Model Integration
  - ISO 27001 – standard for information security
  - ISO 9000 – standard for quality management
  - ISO/IEC 20000 – standard for IT service management
  - ISO 31000:2009 – risk management standard

GEIT Frameworks

  - TOGAF – The Open Group Architecture Framework
  - M_o_R – Management of Risk
  - ITIL – IT Infrastructure Library

- COBIT aligns with the other relevant standards and frameworks at a high level.
- This means that COBIT can be used to be the overarching framework for the governance and management of enterprise IT.

GEIT Frameworks


Evaluate, Direct and Monitor
ISO/IEC 38500
Align, Plan and Organise
TOGAF
ISO/IEC 31000
ISO/IEC 27000
PRINCE2/PMBOK
CMMI
Build, Acquire and Implement
ITIL V3 2011 and ISO/IEC 20000
Deliver, Service and Support
Monitor, Evaluate and Assess

Source: COBIT 5, Figure 25

Business Drivers for IT Governance

- Business drivers constitute the need for IT Governance.
- Typical pain points or trigger events can create the realization that there is a need for improvement.
- IT governance initiates the immediate action to solve or mitigate the pain points and create a platform for further future improvement.

Pain Points

- Typical pain points include :
  - Frustration with failed initiatives, rising IT costs and low business value.
  - Significant incidents related to IT-related business risk, such as data loss or project failure.
  - Outsourcing service delivery service levels not being met.
  - Failure to meet regulatory requirements.
  - IT limiting innovation capability and business agility.

Pain Points

- Regular audit findings of poor IT performance or quality of service.
- Hidden IT spending.
- Duplication or overlap between initiatives and wastage of resources.
- Insufficient IT resources, staff with inadequate skills or dissatisfied employees.
- IT-enabled changes frequently failing to meet business needs and delivered late or over budget.

Pain Points

- Multiple and complex IT assurance efforts.
- Management reluctant to engage with IT or lack of sponsors for IT projects.
- Complex IT operating models, typically decentralized or federated.

Trigger Events

- Other than pain points, internal and external events can trigger a focus on GEIT efforts.
  - Merger, acquisition or divestiture.
  - Shift in market or competition position.
  - New regulatory or compliance requirements.
  - Initiation of an enterprise-wide governance project.
  - New CIO, CFO, CEO or board member.
  - External audit or consultant assessments.

Trigger Events

  - A new business strategy.
  - Desire to significantly improve the value gained from IT.
- Pain points or trigger events provide a starting point from which to commence GEIT initiatives.
- Engaging a third-party to obtain a review may increase buy-in.
- Success of GEIT initiatives depend on participation of everyone in the enterprise.

GEIT Components

- Components interact with one another to support the implementation of a comprehensive governance and management system for GEIT.
- Components are defined as anything that can help achieve the objectives of the enterprise.
- Components can be :
  - Frameworks
  - Principles

GEIT Components

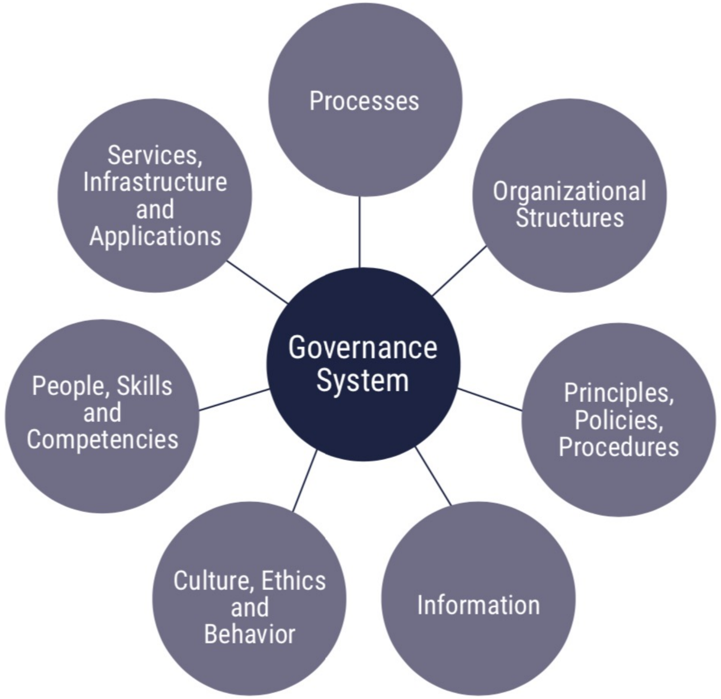
  - Structures
  - Processes
  - Practices
- Key to successful implementation of GEIT is a holistic approach towards the interaction between the components.
- COBIT classifies and identifies 7 key components of achieving GEIT.

GEIT Components

- They are :
    1. Principles, policies and frameworks
    2. Processes
    3. Organizational structures
    4. Culture, ethics and behaviour
    5. Information
    6. Services, infrastructure and applications
    7. People, skills and competencies.

COBIT Components

Figure 4.3—COBIT Components of a Governance System


Processes
Services, Infrastructure and Applications
Organizational Structures
Governance System
People, Skills and Competencies
Principles, Policies, Procedures
Culture, Ethics and Behavior
Information

COBIT 2019

IT Strategy

- It is important to identify IT strategy in implementing GEIT.
- IT strategy needs to be aligned to the enterprise’s mission, vision and values.
- Techniques to identify strategy include:
    - Strengths, Weaknesses, Opportunities and Threats (SWOT)
    - BCG matrix

SWOT Analysis

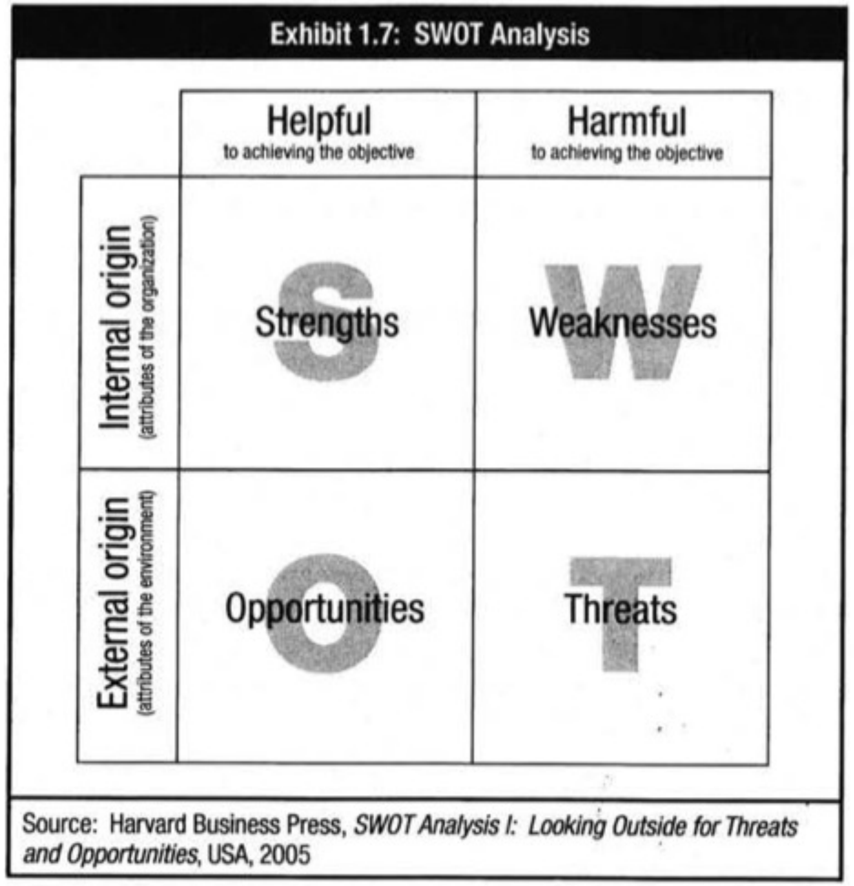


Exhibit 1.7: SWOT Analysis

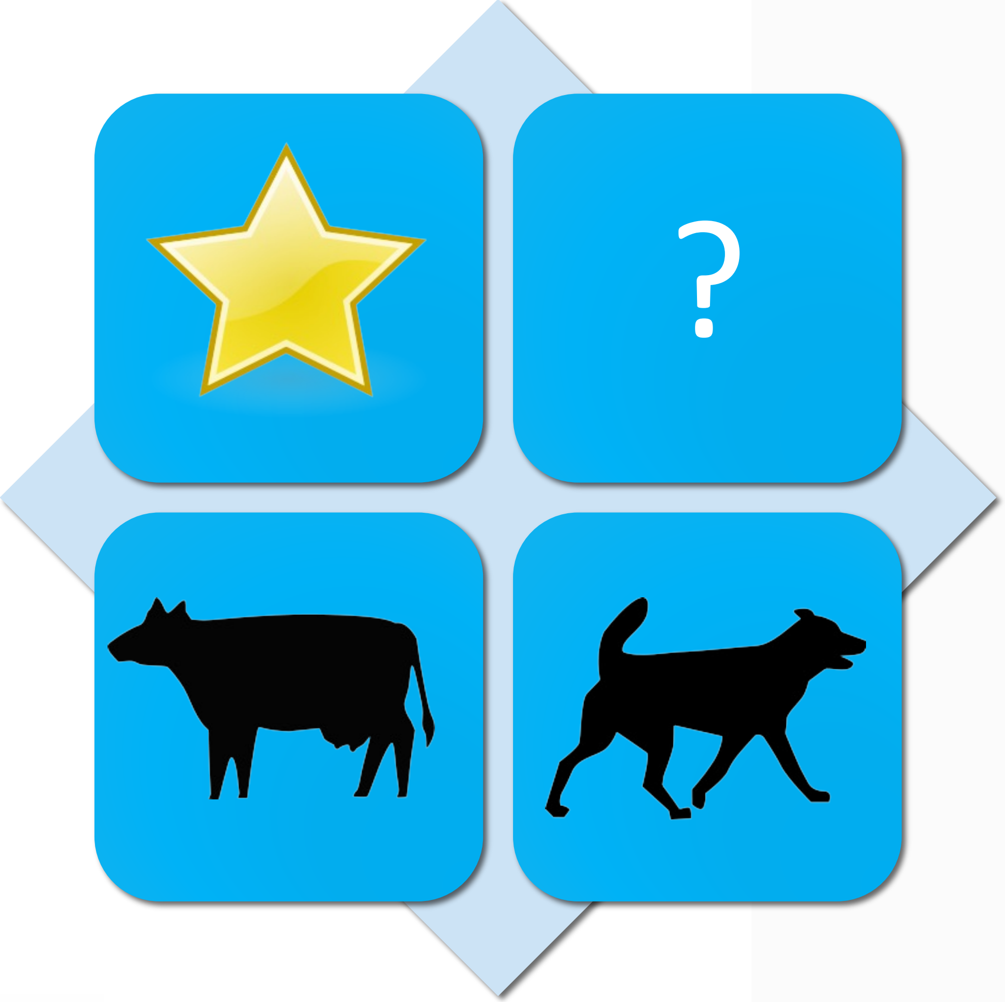
	Helpful to achieving the objective	Harmful to achieving the objective
Internal origin (attributes of the organization)	Strengths	Weaknesses
External origin (attributes of the environment)	Opportunities	Threats

Source: Harvard Business Press, *SWOT Analysis I: Looking Outside for Threats and Opportunities*, USA, 2005

SWOT Analysis is a tool that can be used by the organization to identify its:

- **Strengths**, so that it may continue to develop them,
- **Weaknesses**, so that it can mitigate them,
- **Opportunities**, so that they can be developed into future strengths,
- **Threats**, so that they can be addressed before they become a more serious issue.

BCG Matrix



Developed by the Boston Consulting Group (BCG), the BCG Matrix is similar to the SWOT Analysis tool.

It identifies the following:

- **Stars** : Also known as cash cows. They can generate a lot of returns and bring about the most benefit to the organization. Should be maintained or developed further.
- **Dog** : Area which do not take up a lot of resources but neither do they generate a lot of benefits
- **Stars** : Area which take up a lot of resources but do not produce a lot of returns either. Need to develop them into cash cows.
- **Question mark** : Area which has potential to become cash cows. Although it is not generating a lot of benefits, it has the potential to, with sufficient investment.

Organizational Structures

- Effective governance of enterprise IT requires that IT-related decisions are made in a transparent manner and effective communication between business and IT management is a must.
- Organizational structures are important elements in ensuring that this is done.
- Organizational structures is specified as an enabler in COBIT.

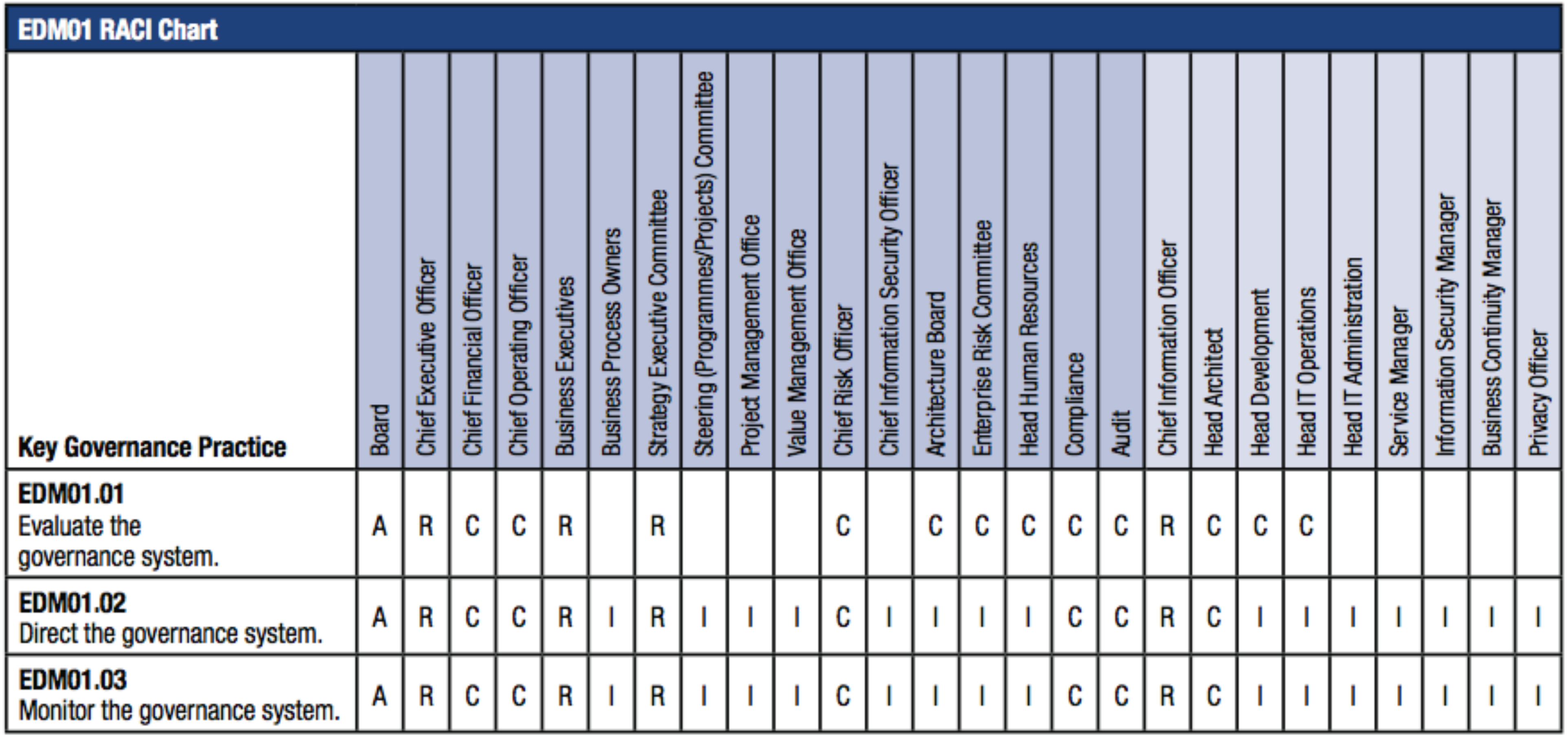
Roles and Org Structures

Role / Structure	Definition / Description
Board	The group of the most senior executives and/or non-executive directors of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources
CEO	The highest-ranking officer who is in charge of the total management of the enterprise
CFO	The most senior official of the enterprise who is accountable for all aspects of financial management, including financial risk and controls and reliable and accurate accounts
COO	The most senior official of the enterprise who is accountable for the operation of the enterprise
CRO	The most senior official of the enterprise who is accountable for all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk
CIO	The most senior official of the enterprise who is responsible for aligning IT and business strategies and accountable for planning, resourcing and managing the delivery of IT services and solutions to support enterprise objectives
CISO	The most senior official of the enterprise who is accountable for the security of enterprise informaiton in all its forms
Business Executive	A senior management individual accountable for the operation of a specific business unit or subsidiary

Roles and Org Structures

- There are many other roles defined in COBIT which are relevant to GEIT.
- Not all need to be specifically present, but a position/person within the organization should be able to identify with the various roles.
- COBIT includes a RACI (Responsible, Accountable, Consulted and Informed) chart to link a process to various roles.

RACI Chart



EDM01 RACI Chart

Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM01.01 Evaluate the governance system.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Direct the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Monitor the governance system.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

RACI Chart

- In COBIT, a RACI chart shows the assignment of various governance responsibilities to various roles in the organisation.
- Effective governance is dependent on comprehensive allocation of responsibilities to provide end-to-end coverage of all governance activities.

Conclusion

- Frameworks such as COBIT provide the structure through which GEIT is effectively implemented.
- Other frameworks which deal with specific IT practices can be integrated into Governance Frameworks to provide a holistic approach towards GEIT.
- Management techniques help to support governance practices.