Governance SPICE

Using COSO and COBIT

Process Assessment Models

Linking Governance to Sustainable Value Creation

BPM GOSPEL

(LLP-LDV-TOI-2010-HU-001)

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

János Ivanyos
Memolux Ltd.
ivanyos@memolux.hu

Dr. József Roóz
Budapest Business School
rooz.jozsef@bgf.hu

Workshop Community: SPICE Assessors - Exchanging Experiences across Assessment Models
18th EuroSPI Conference, Roskilde University, Denmark, 27 - 29 June 2011

Topics

- ”Governance” SPICE (2005-2012)
- COBIT/COSO Performance Measurement
- Governance Capability - Mapping COSO Objectives with ISO/IEC 15504 Capability Levels
- COSO & COBIT as Process Reference Models
- Linking Governance to Sustainable Value Creation
  - Governance Model for Trusted Businesses
  - Multi-layer business assurance technology
  - Developing case studies for learning and coaching

”Governance” SPICE (2005-2012)

Refers to

- Governance, Risk and Controls (OECD Principles, Regulations, Audit Standards)

based on different concepts (IA-Manager 2005-2007)

- Recognized Control Frameworks (COSO&COBIT)
- Risk Tolerance and Risk Appetite (COSO ERM)
- Performance Measurement (COBIT)
- Process Capability Assessment (ISO/IEC 15504-2)
- Evaluating Process-related Risk (ISO/IEC 15504-4)
- Organizational Maturity (ISO/IEC TR 15504-7)

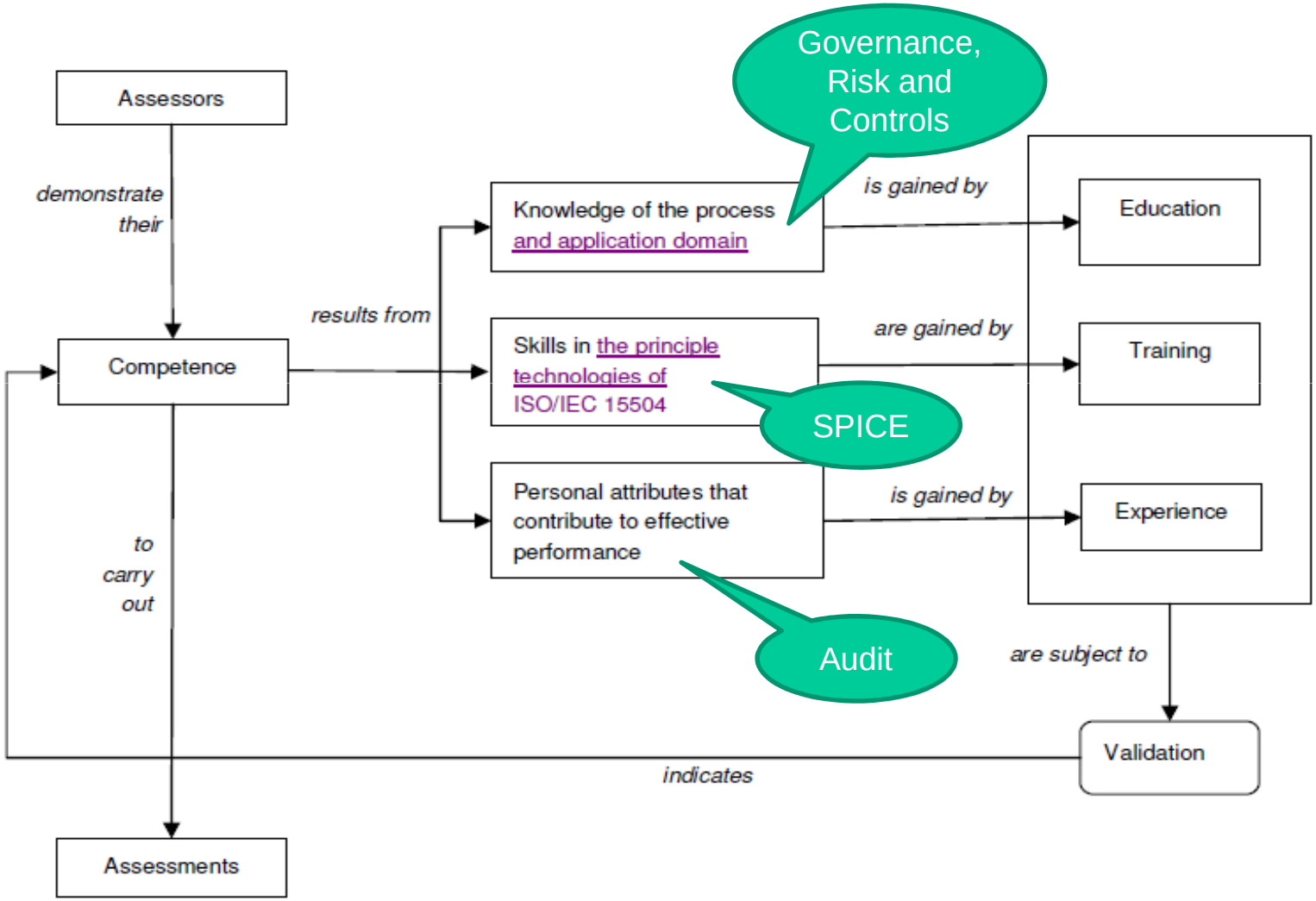
by using multilingual ontology (MONTIFIC 2008-2010)

- Terminology database
- Ontology model

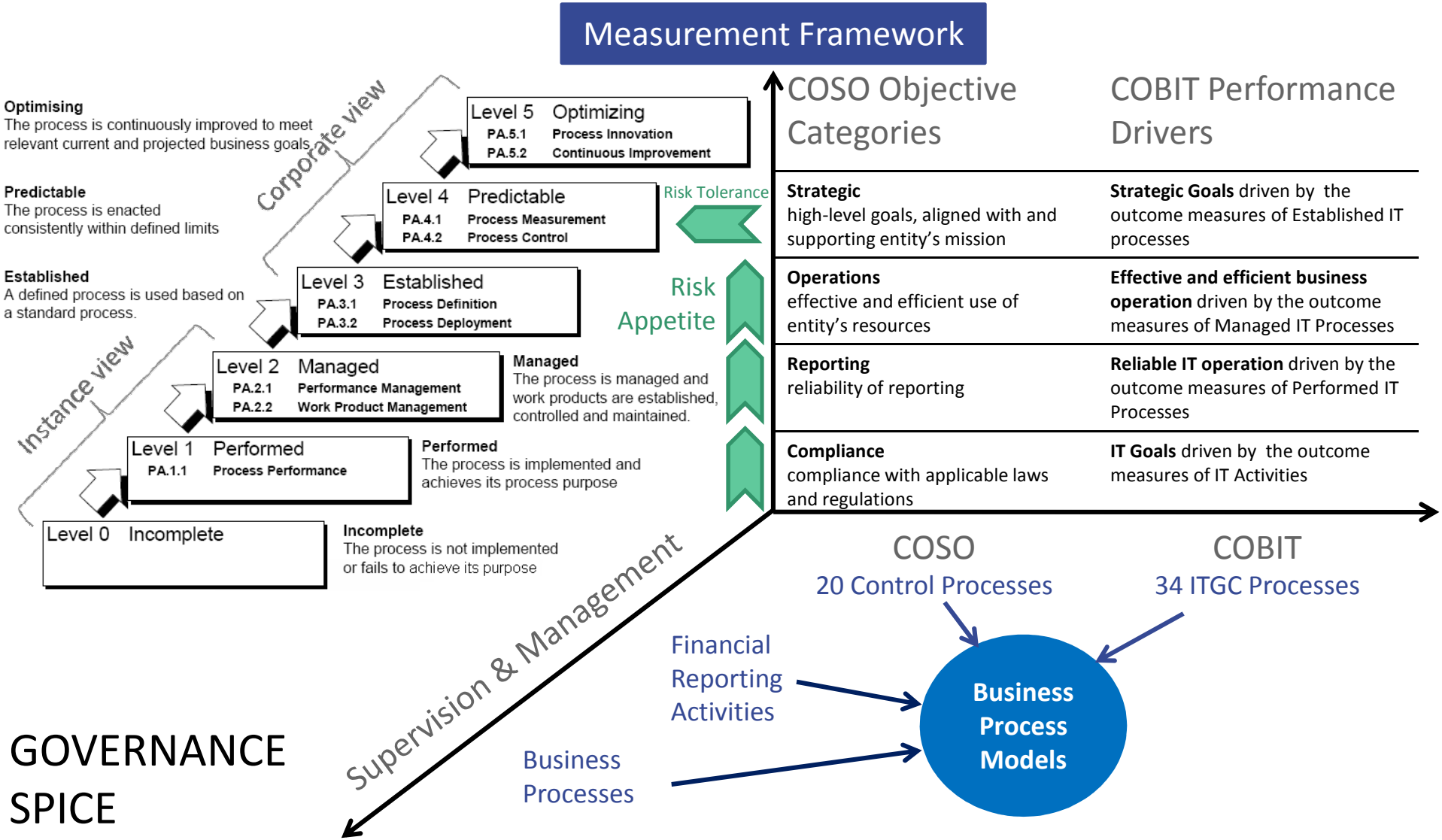
to leverage sustainable value creation (GOSPEL 2010-2012)

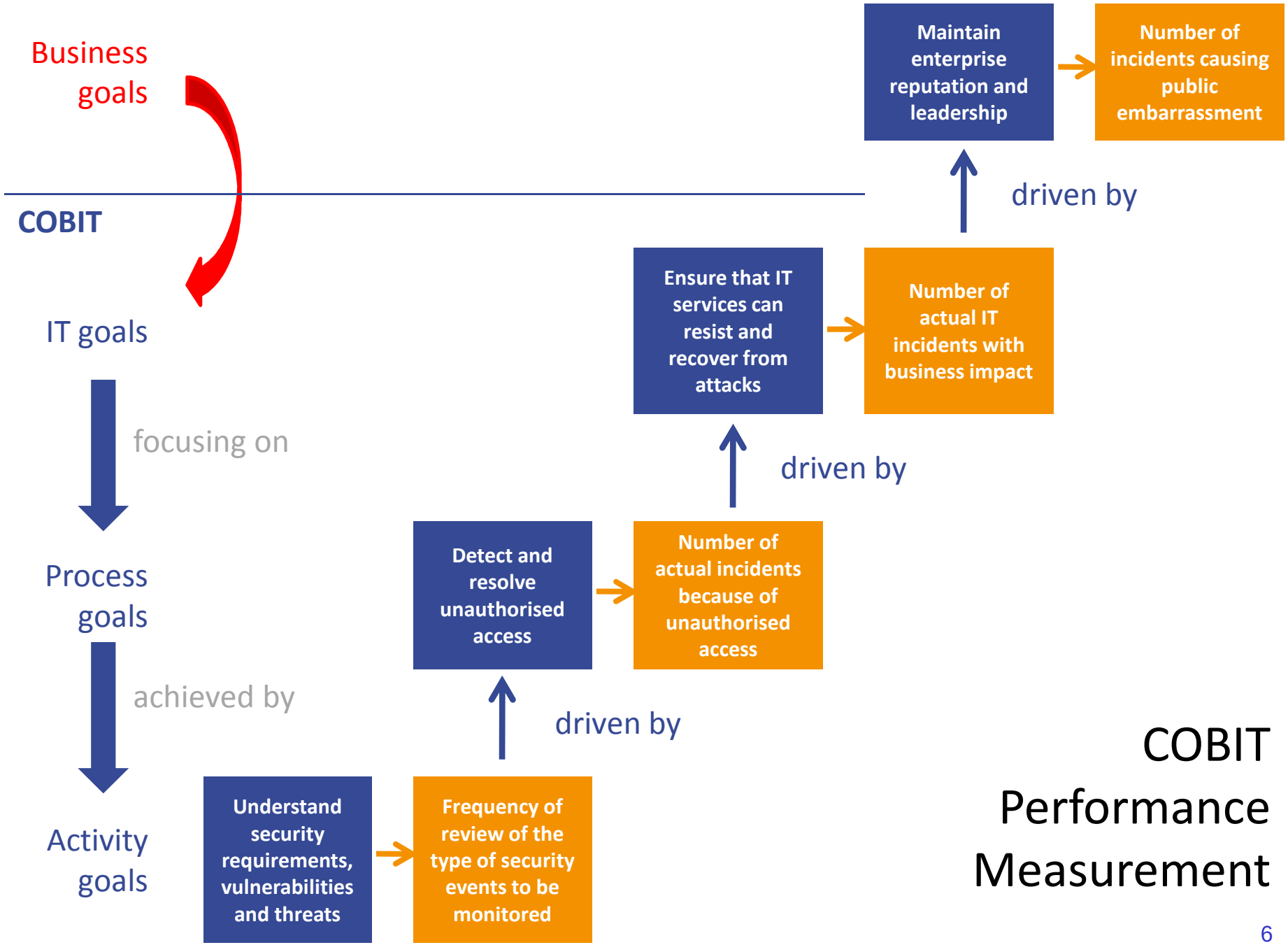
- Governance Model for Trusted Businesses
- Multi-layer business assurance technology

Validation of Governance SPICE Competencies



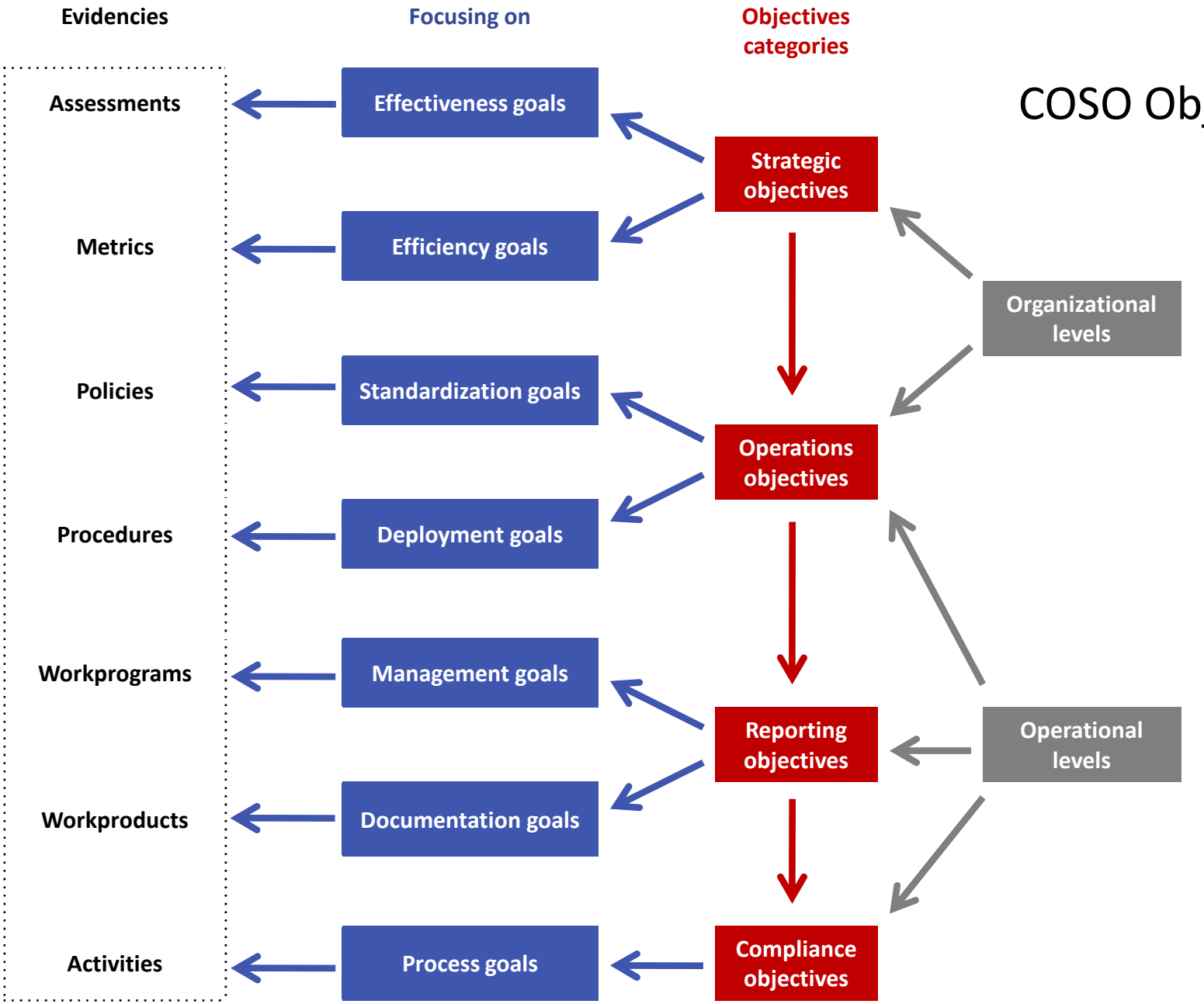
Using COSO & COBIT Process Assessment Models



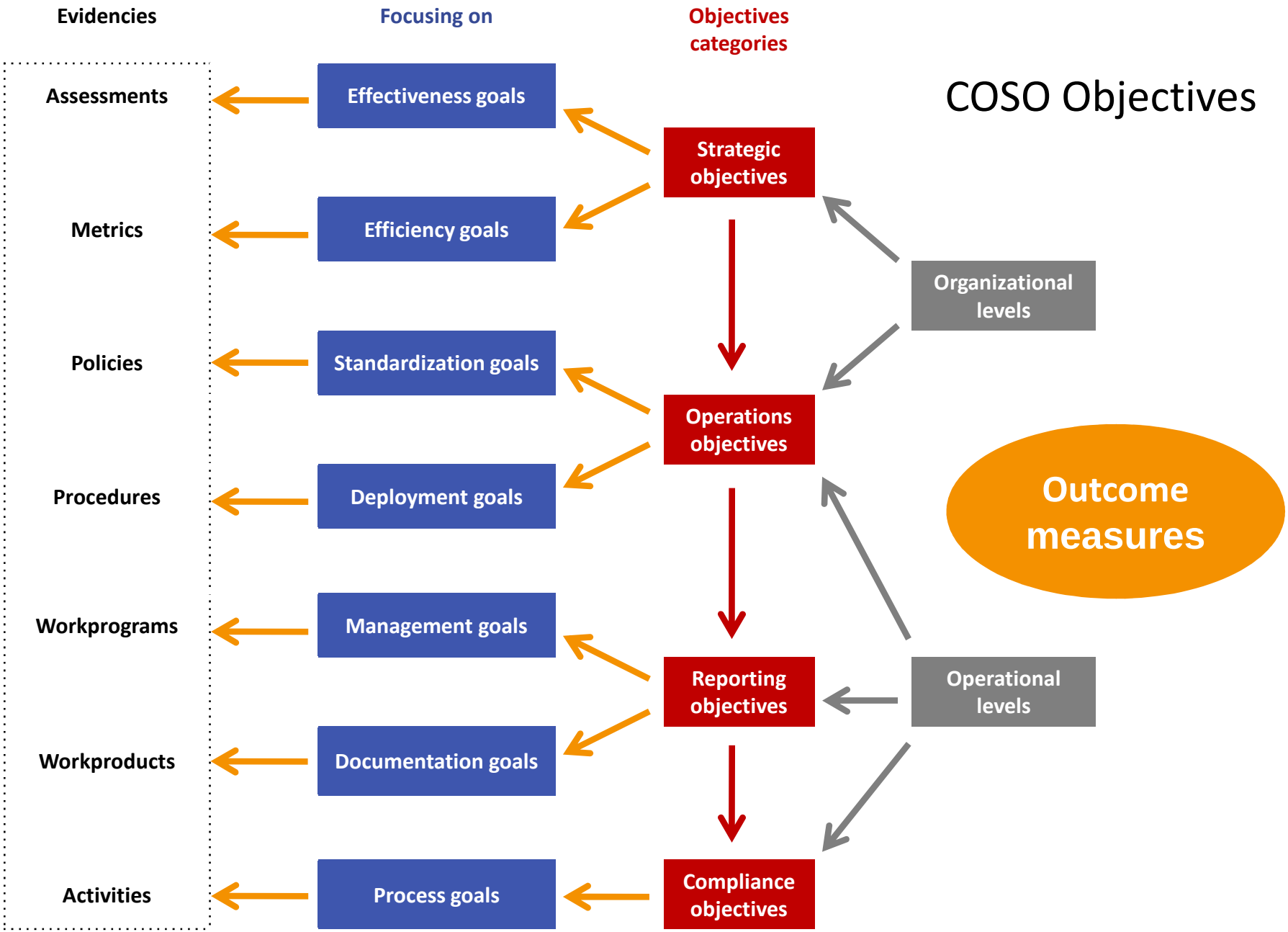


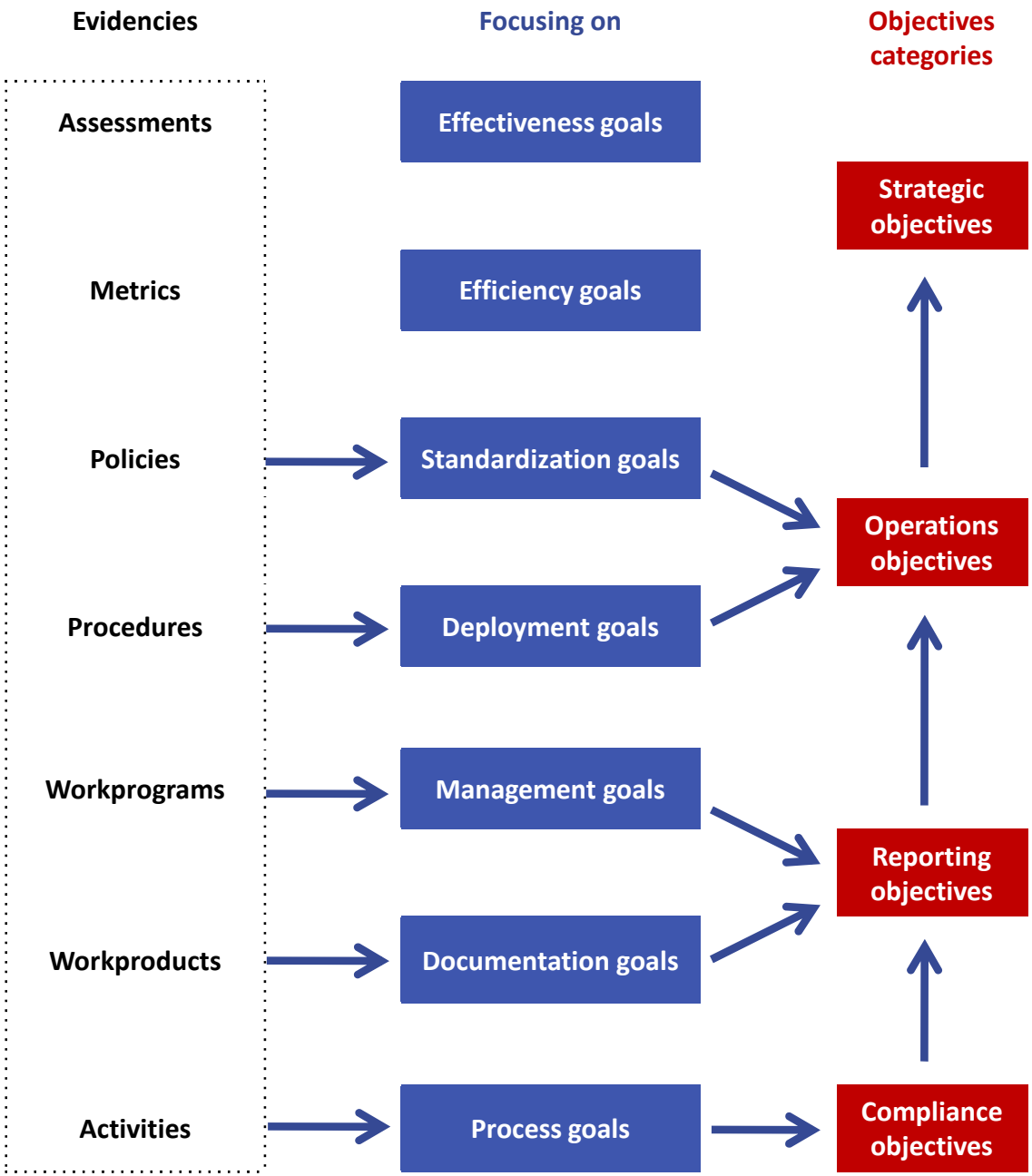
COBIT Performance Measurement

COSO Objectives



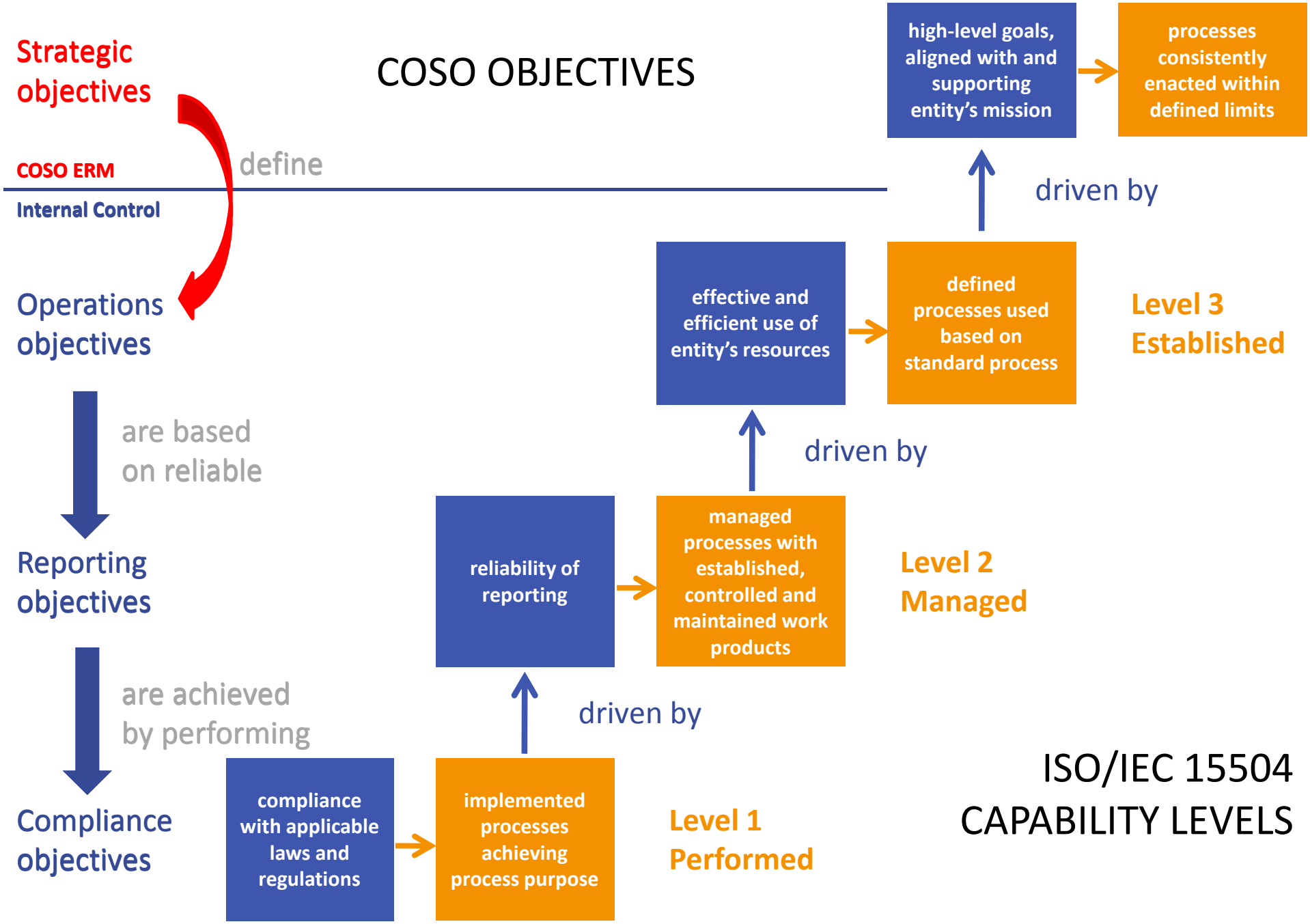
COSO Objectives





COSO Objectives

Performance drivers


COSO OBJECTIVES
Strategic objectives
define
COSO ERM
Internal Control
Operations objectives
are based on reliable
Reporting objectives
are achieved by performing
Compliance objectives
high-level goals, aligned with and supporting entity's mission
processes consistently enacted within defined limits
driven by
effective and efficient use of entity's resources
defined processes used based on standard process
Level 3 Established
driven by
reliability of reporting
managed processes with established, controlled and maintained work products
Level 2 Managed
driven by
compliance with applicable laws and regulations
implemented processes achieving process purpose
Level 1 Performed
ISO/IEC 15504 CAPABILITY LEVELS

ISO/IEC 15504 Capability Levels

The process is continuously improved to meet relevant current and projected business goals.

Level 5 Optimizing process
PA 5.1 Process Innovation
PA 5.2 Process Optimization

The process is enacted consistently within defined limits.

Level 4 Predictable process
PA 4.1 Process Measurement
PA 4.2 Process Control

A defined process is used based on a standard process.

Level 3 Established process
PA 3.1 Process Definition
PA 3.2 Process Deployment

Level 2 Managed process
PA 2.1 Performance Management
PA 2.2 Work Product Management

The process is managed and work products are established, controlled and maintained.

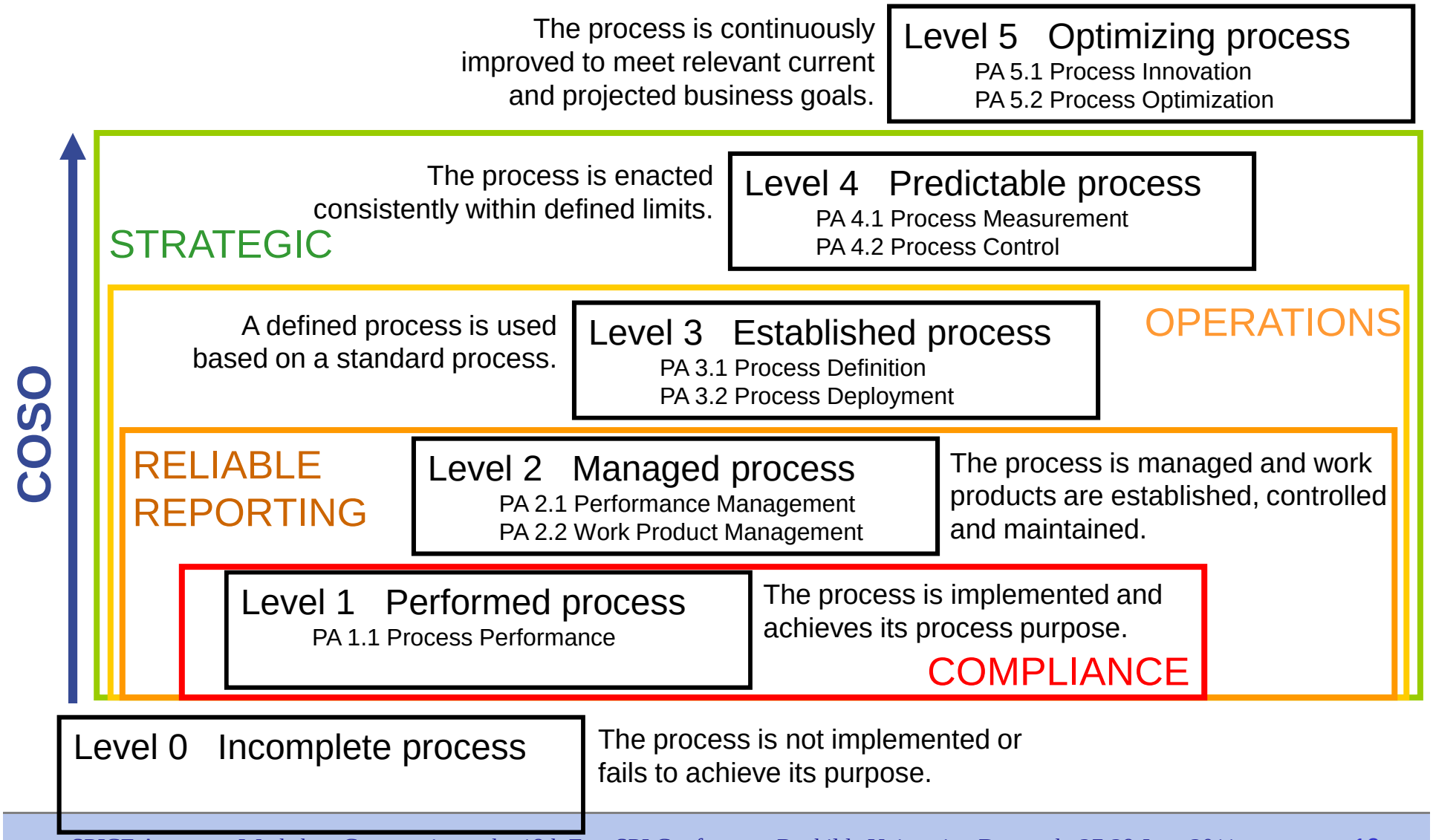
Level 1 Performed process
PA 1.1 Process Performance

The process is implemented and achieves its process purpose.

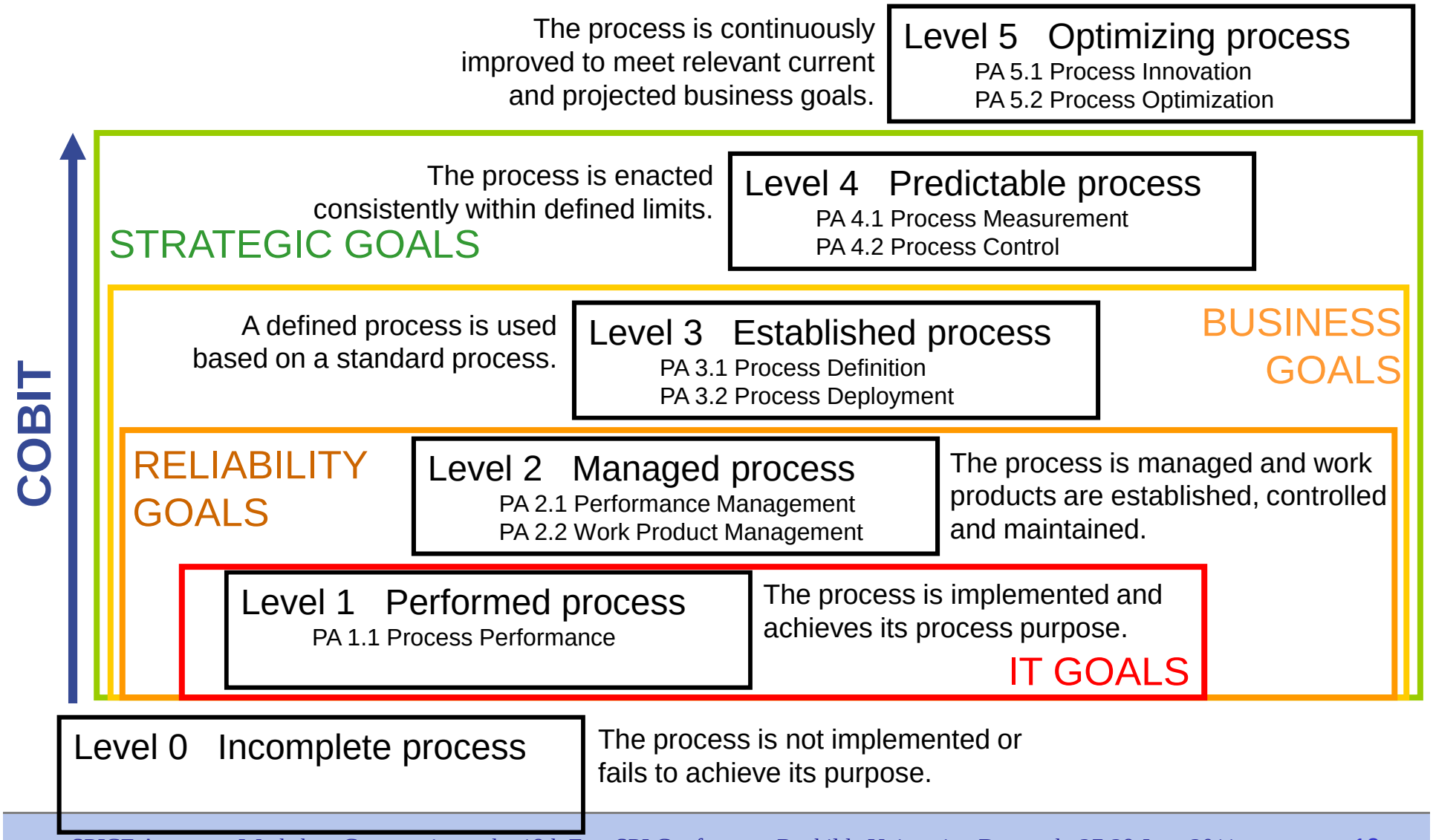
Level 0 Incomplete process

The process is not implemented or fails to achieve its purpose.

ISO/IEC 15504 Capability Levels and COSO



ISO/IEC 15504 Capability Levels and COBIT



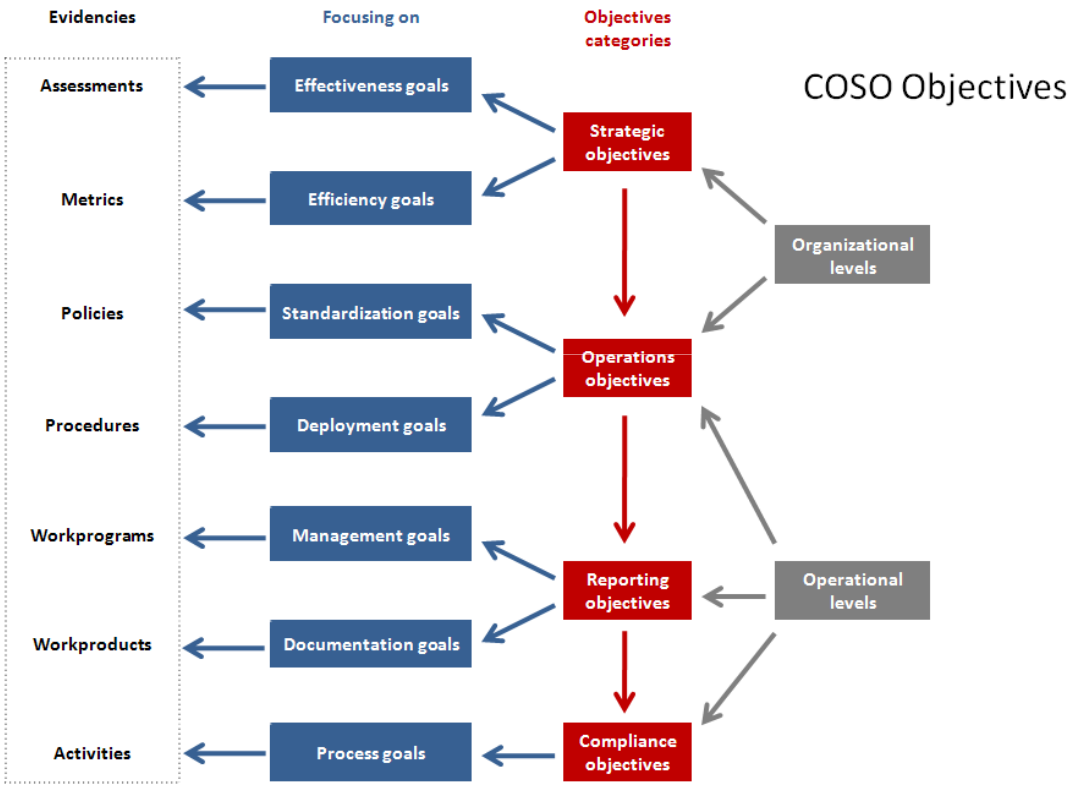
Mapping Objectives' Outcome Measures with Capability Levels

Level 4 Predictable process
- PA 4.1 Process Measurement
- PA 4.2 Process Control

Level 3 Established process
- PA 3.1 Process Definition
- PA 3.2 Process Deployment

Level 2 Managed process
- PA 2.1 Performance Management
- PA 2.2 Work Product Management

Level 1 Performed process
- PA 1.1 Process Performance



Terminology Mapping

ISO/IEC 15504	COSO	COBIT
Process Category	Component	Domain
Process	Principle	Process
Process Name	Principle name	Process name
Process Purpose	Principle description	IT goal
Process Outcome	Attribute	Activity goal
Base Practice	Approach	Control Objective
Work Product	-	Input/Output

COBIT processes

Plan and Organize (PO)

- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organisation and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks
- PO10 Manage Projects

Acquire and Implement (AI)

- 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
- AI7 Install and Accredit Solutions and Changes

Deliver and Support (DS)

- DS1 Define and Manage Service Levels
- DS2 Manage Third-party Services
- DS3 Manage Performance and Capacity
- DS4 Ensure Continuous Service
- DS5 Ensure Systems Security
- DS6 Identify and Allocate Costs
- DS7 Educate and Train Users
- DS8 Manage Service Desk and Incidents
- DS9 Manage the Configuration
- DS10 Manage Problems
- DS11 Manage Data
- DS12 Manage the Physical Environment
- DS13 Manage Operations

Monitor and Evaluate (MO)

- ME1 Monitor and Evaluate IT Performance
- ME2 Monitor and Evaluate Internal Control
- ME3 Ensure Compliance With External Requirements
- ME4 Provide IT Governance

COSO processes

Control Environment (CE)

- Integrity and Ethical Values (IEV)
- Oversight Board (OB)
- Management's Philosophy and Operating Style (MPO)
- Organizational Structure (OS)
- Financial Reporting Competencies (FRC)
- Authority and Responsibility (AR)
- Human Resources (HR)

Risk Assessment (RA)

- Financial Reporting Objectives (FRO)
- Financial Reporting Risks (FRR)
- Fraud Risk (FR)

Control Activities (CA)

- Integration with Risk Assessment (IRA)
- Selection and Development of Control Activities (SD)
- Policies and Procedures (PD)
- Information Technology (IT)

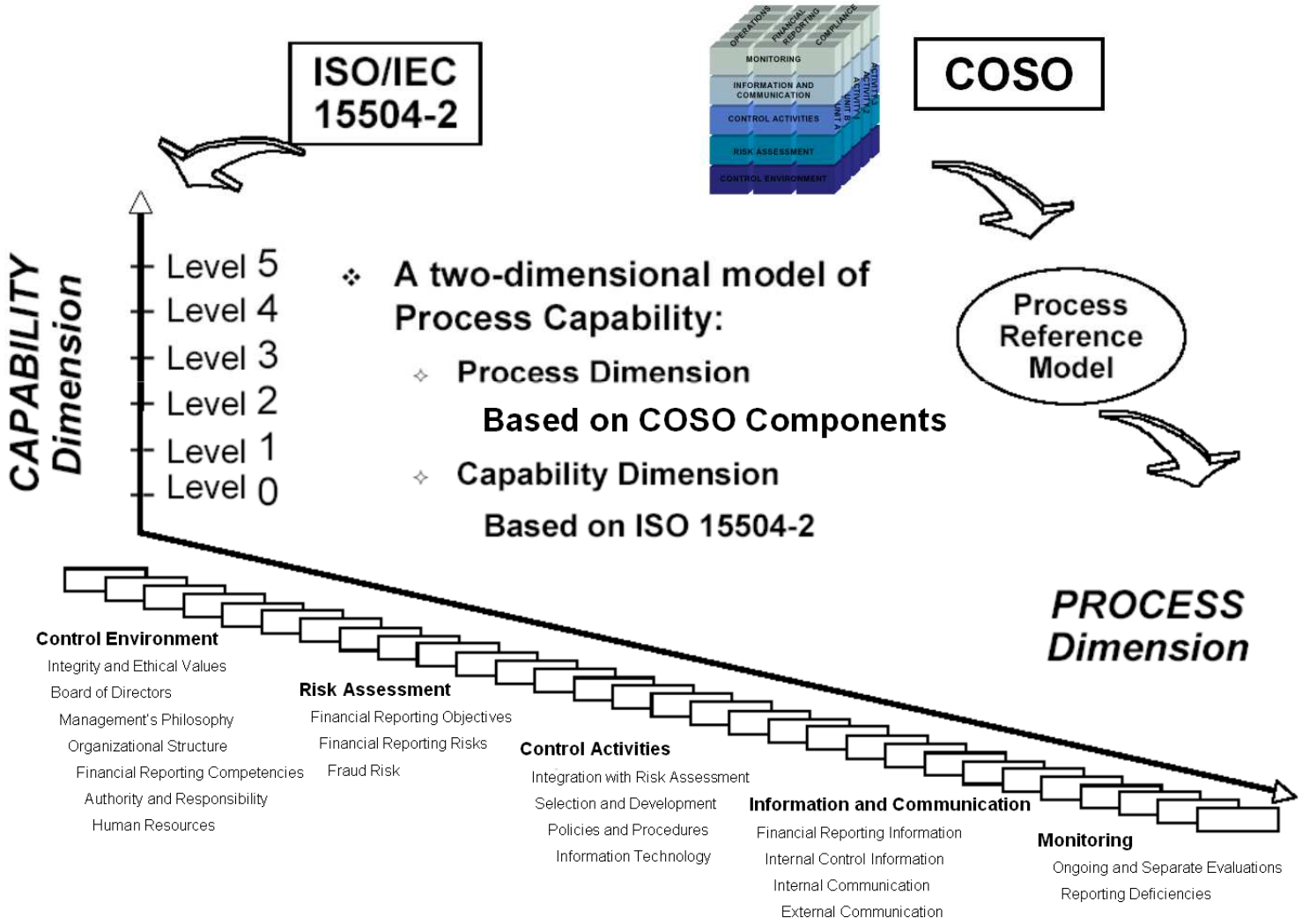
Information and Communication (IC)

- Financial Reporting Information (FRI)
- Internal Control Information (ICI)
- Internal Communication (IC)
- External Communication (EC)

Monitoring (MO)

- Ongoing and Separate Evaluations (OSE)
- Reporting Deficiencies (RD)

COSO-based Process Assessment Model



ISO/IEC 15504 conform process definition of a COSO Principle

Process ID	**IFC.CE.IEV**
Process Name	**Integrity and Ethical Values**
Process Purpose	Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.
Process Outcomes	As a result of successful implementation of IFC.CE.IEV process: **1) Values articulated** – Top management develops a clearly articulated statement of ethical values that is understood at all levels of the organization. **2) Adherence monitored** – Processes are in place to monitor adherence to principles of sound integrity and ethical values. **3) Deviation addressed** – Deviations from sound integrity and ethical values are identified in a timely manner and appropriately addressed and remedied at appropriate levels within the organisation.

ISO/IEC 15504 conform base practice descriptions from COSO

Base Practices	**IFC.CE.IEV.BP1 Articulate and Demonstrate Integrity and Ethics** The key members of management articulate and demonstrate the importance of sound integrity and ethical values to employees. [Outcomes: 1, 2, 3] NOTE: Management can perform this practice through their: • Day-to-day actions and decision-making. • Interactions with suppliers, customers, and other external parties that reflect fair and honest dealings. • Performance appraisals and incentives that diminish temptations inconsistent with financial reporting objectives. • Intolerance of ethical violations at all levels. **IFC.CE.IEV.BP2 Inform Employees about Integrity and Ethics** Management implements mechanisms to inform new employees and remind current personnel of the organisation's objectives related to integrity and ethics and related corporate values. [Outcomes: 1, 2]

ISO/IEC 15504 conform definition of a COBIT process

Control over the IT process of

Define a strategic IT plan

Process

that satisfies the business requirement for IT of

sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks

Purpose

by focusing on

incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner

Related Practices

is achieved by

Engaging with business and senior management in aligning IT strategic planning with current and future business needs
Understanding current IT capabilities
Providing for a prioritisation scheme for the business objectives that quantifies the business requirements

Outcomes

and is measured by

Percent of IT objectives in the IT strategic plan that support the strategic business plan
Percent of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plans
Delay between updates of IT strategic plan and updates of IT tactical plans

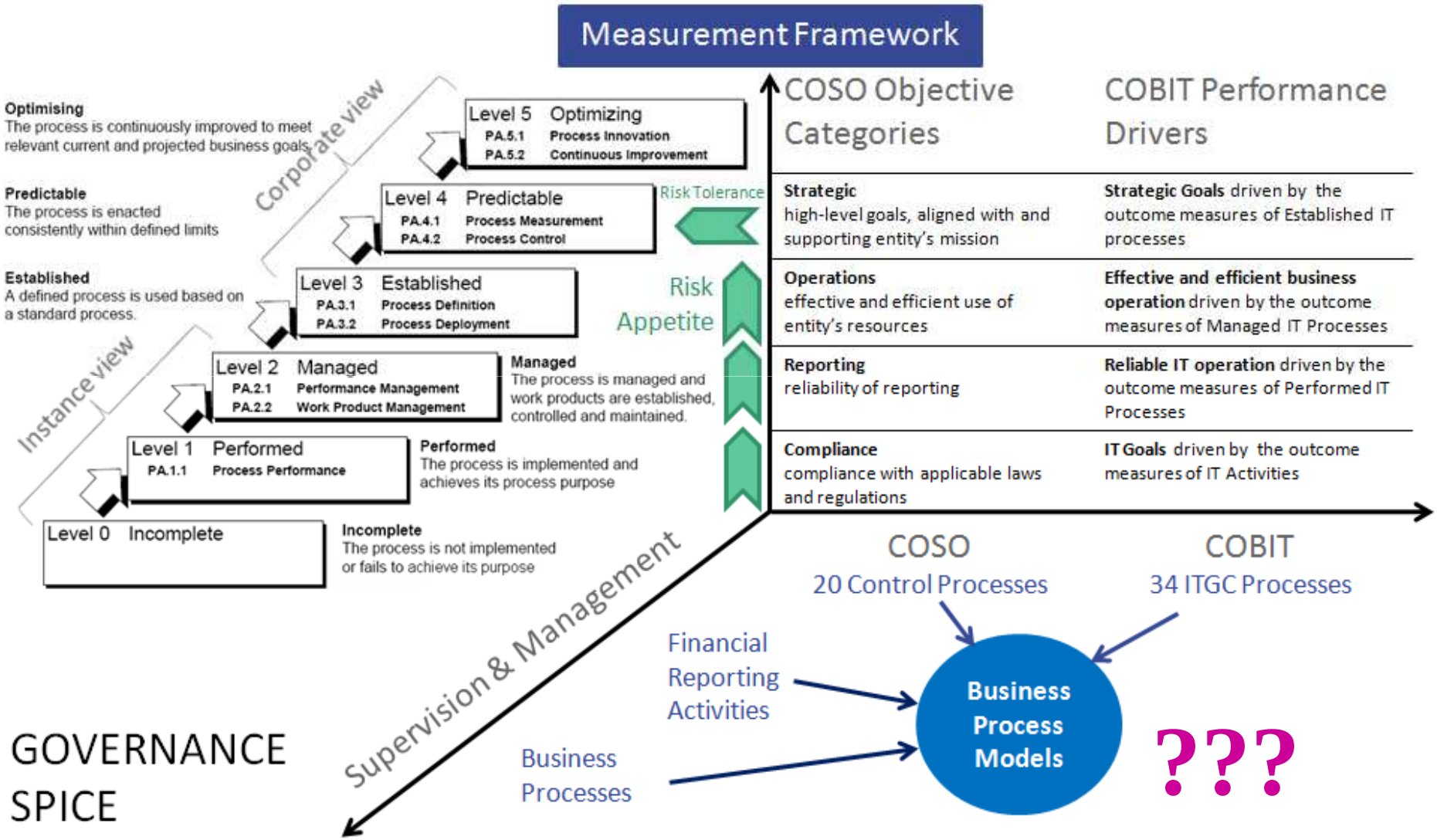
COBIT PAM (Exposure Draft 12 Apr 2011)

COBIT® Assessment Process (CAP): COBIT® 4.1 Process Assessment Model

3.1 Plan and Organise (PO)

Process ID / Process Name	PO1 Define a Strategic IT Plan		
Purpose	Satisfy the business requirement of sustaining or extending the business strategy and governance requirements while being transparent about benefits, costs and risks.		
Outcomes (Os)	Number	Description	
	PO1-O1	Value management processes, including business cases and benefits realisation, are established.	
	PO1-O2	Business and IT are involved in strategic planning.	
	PO1-O3	Current IT capabilities are defined.	
	PO1-O4	An IT strategic plan is prepared that defines IT goals and priorities based on the business objectives.	
	PO1-O5	IT tactical plans are prepared.	
	PO1-O6	Project and service portfolios are prepared and managed.	
Base Practices (BPs)	Number	Description	Supports
	PO1-BP1	Link business goals to IT goals.	PO1-O1, O2
	PO1-BP2a	Identify critical dependencies.	PO1-O2, O6
	PO1-BP2b	Identify current performance.	PO1-O3
	PO1-BP3	Build an IT strategic plan.	PO1-O2, O4
	PO1-BP4	Build IT tactical plans, taking into account dependencies and performance identified.	PO1-O5
	PO1-BP5a	Analyse program portfolios.	PO1-O6
	PO1-BP5b	Manage project and service portfolios.	PO1-O6
Work Products (WPs)			
Inputs			
Number	Description		Supports
PO5-WP1	Cost-benefit reports		PO1-O1, O4
PO9-WP1	Risk assessment		PO1-O1, O3, O4, O5
PO10-WP5	Updated IT project portfolio		PO1-O6
DS1-WP3	New/updated service requirements		PO1-O6
DS1-WP6	Updated IT service portfolio		PO1-O6
Outside COBIT	Business strategy and priorities		PO1-O2, O4
Outside COBIT	Programme portfolio		PO1-O1, O6
ME1-WP1	Performance input to IT planning		PO1-O5
ME4-WP2	Report on IT governance status		PO1-O1, O2
ME4-WP4	Enterprise strategic direction for IT		PO1-O1, O2

Linking Governance to Sustainable Value Creation



Setting Governance Objectives

- Supporting Organization's Internal Control System
  - Risk Awareness
  - Accountability
  - Competency
  - Accuracy
  - Process Integrity
  - Data Protection
  - Commitment
  - Control Efficiency
- Supporting Business Sustainability
  - Competitiveness
  - Exploitability
  - Satisfaction

Determining Application Process for a Governance Objective (Accuracy)

Governance Objective	Key Risk	Risk Factors	Responses	Applicable COSO&COBIT processes	Application Practices
4. Accuracy / Information Reliability Ensured	Inconsistency in data architecture and disclosure elements	Information architecture is inconsistent with processing requirements	Maintaining effective information architecture and data model	**Define the Information Architecture (COBIT)**	Satisfy the business requirement of being agile in responding to requirements; provide reliable, consistent information, and seamlessly integrate applications into business processes.
		Non-compliance with rules and regulations are not detected in time	Information is systematically collected and assessed to detect compliance issues, privacy problems and fraud	**Financial Reporting Information (COSO)**	Pertinent information is identified, captured, used at all levels of the organisation, and distributed in a form and timeframe that supports the achievement of the organization's financial reporting and trusted business objectives.
		Availability and quality of control information are not sufficient	Control information for automated process settings, data manipulations and calculations are maintained systematically	**Internal Control Information (COSO)**	Information used to execute other control components is identified, captured, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities.

Information Reliability – Governance Process (Accuracy Objective)

Process ID	GOV.IR
Process Name	Information Reliability
Process Purpose	The purpose of the Information Reliability process is to ensure the accuracy and consistency in data architecture and disclosure elements relevant for financial reporting and trusted business objectives, and for supporting data processing integrity. NOTE1: The Information Reliability process is **a special application** of the COSO 2006 and COBIT 4.1 models in the context of the "**Accuracy**" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles and the COBIT 4.1 framework in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 and COBIT 4.1 based reference models without recreating processes that are already well established. NOTE2: The descriptions of the COBIT 4.1 processes and the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference models and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard.
Process Outcomes	As a result of successful implementation of the Information Reliability process the following service governance objectives are achieved: 1) Effective information architecture and data model are maintained. 2) Information is systematically collected and assessed to detect compliance issues, privacy problems and fraud. 3) Control information for automated process settings, data manipulations and calculations are maintained systematically.

Using ”Define the Information Architecture” COBIT Process as an Application Practice

Application practice	**AP01 Ensure the integrity and consistency of all data stored in electronic form.** Satisfy the business requirement of being agile in responding to requirements; provide reliable, consistent information, and seamlessly integrate applications into business processes. [Outcome: 1] NOTE1: This practice is implemented by performing practices (control objectives) of the COBIT 4.1 Define the Information Architecture process with a specific focus on how governance supports internal control over financial reporting and business operation: **PO2.1 Create and maintain enterprise information model.** Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure. **PO2.2 Create and maintain enterprise data dictionary (ies).** Maintain an enterprise data dictionary that incorporates the organisation’s data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created. **PO2.3 Establish and maintain data classification scheme.** Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption. **PO2.4 Manage data integrity.** Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.

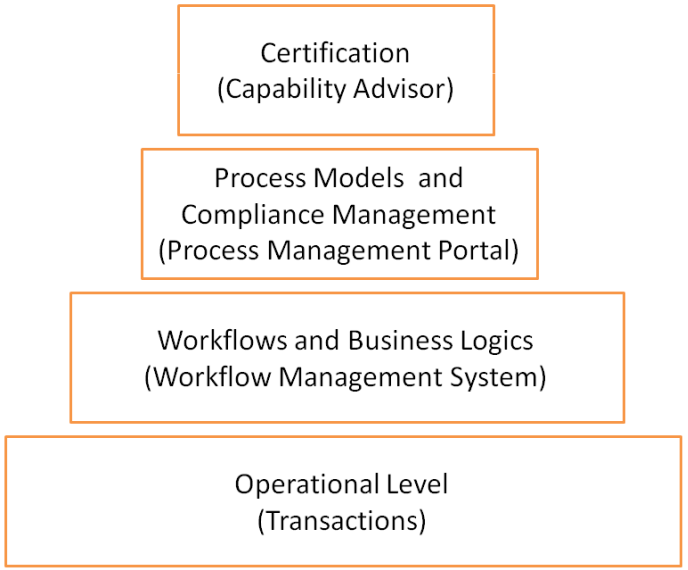
Information Reliability - Governance Process using COSO&COBIT

Relationship Notes	The relationships between the **Information Reliability process and application practices**, and other processes in COSO 2006 and COBIT 4.1 models, have been noted for each practice above. **This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.** (Like in Enterprise SPICE)
Sources	**COBIT 4.1:** PO2 Define the Information Architecture **COSO 2006:** IFC.IC.FRI Financial Reporting Information, IFC.IC.ICI Internal Control Information
References	**Control Objectives for Information and related Technology - COBIT® 4.1** Copyright © 2007 by the IT Governance Institute. 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA. All rights reserved. **Internal Control over Financial Reporting — Guidance for Smaller Public Companies** Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved.

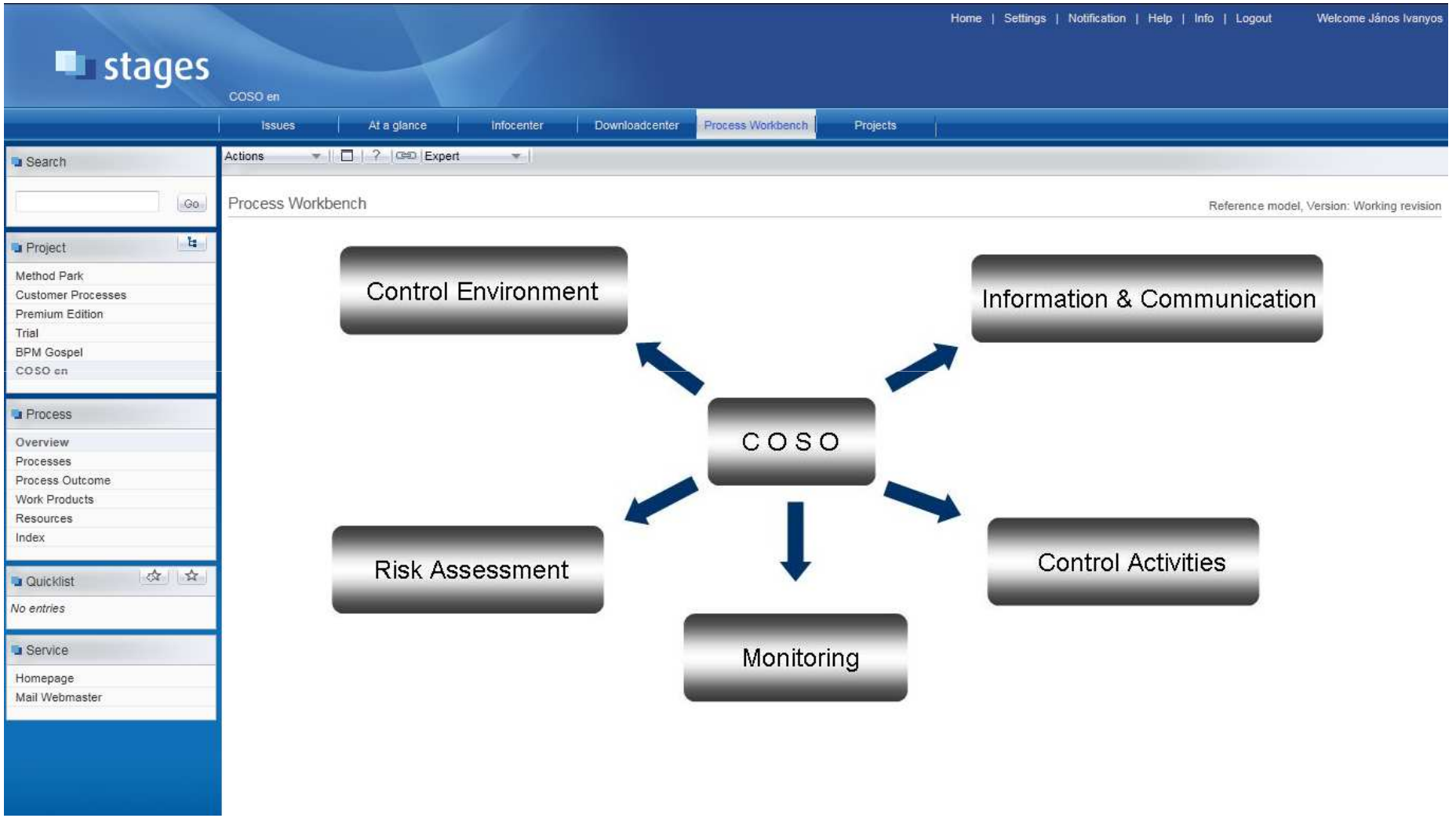
BPM GOSPEL: Multi-layer business assurance technology

Concept of 4 layers in BPM GOSPEL:

- Transaction Processing – Memolux Payroll system
- Workflow/Control Management – ADAMAS by GEMMA Ltd.
- Compliance/Audit Management – Stages ”Governance” Edition by Method Park AG
- Certification – Capability Advisor by ISCN



Using Stages ”Governance” Edition for Compliance/Audit Management



BPM GOSPEL Case Studies (by end of 2011)

Different approaches for demonstrating added business value are considered

- per industry needs mapping them to Governance objectives, for example:
  - Memolux payroll SOC1&SOC2
  - Gemma – ESF grant management
  - Method Park - Business SPICE for big company
  - BBS - Short Cycle Higher Education
  - ISCN - ECQA Job-role Committee management
- per (set of) governance objectives
  - Top five based on presentable added values
- Participation interest from workshop community is welcome!

Topics covered

- ”Governance” SPICE (2005-2012)
- COBIT/COSO Performance Measurement
- Governance Capability - Mapping COSO Objectives with ISO/IEC 15504 Capability Levels
- COSO & COBIT as Process Reference Models
- Linking Governance to Sustainable Value Creation
  - Governance Model for Trusted Businesses
  - Multi-layer business assurance technology
  - Developing case studies for learning and coaching

More information: www.ia-manager.org

Thank you for your attention!