Governance SPICE

Applying Integrated Risk Management Scenarios for Better Controls at SMEs

.

János Ivanyos
Budapest Business School
ivanyos@trusted.hu

HARBIF International Workshop, Budapest Business School, Budapest, Hungary, 4 April 2014

The Governance SPICE Roadmap (2005-2013)

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 for training

to leverage sustainable value creation (BPM-GOSPEL 2010-2013)

- New ”Trusted Business Model” and extension of Governance SPICE Assessor Skill Card
- Multi-layer business assurance technology supporting coaching (assessor training) programs

The Governance SPICE Roadmap (2013-2015)

HARBIF Project (2013-2015)

- HOLISTIC APPROACH TO RISK – BASED INTERNAL FINANCIAL CONTROL FOR SMEs
- Co-funded by the European Commission under the LLP Leonardo da Vinci Programme (Contract No: 2013-TR1-LEO05-47517)
- Turkish, Slovene, Lithuanian and Hungarian partners

based on previous project results

- Internal Financial Control Assessor & Governance SPICE Assessor skillcards
- E-learning contents (www.ia-manager.org)
- ECQA certification scheme

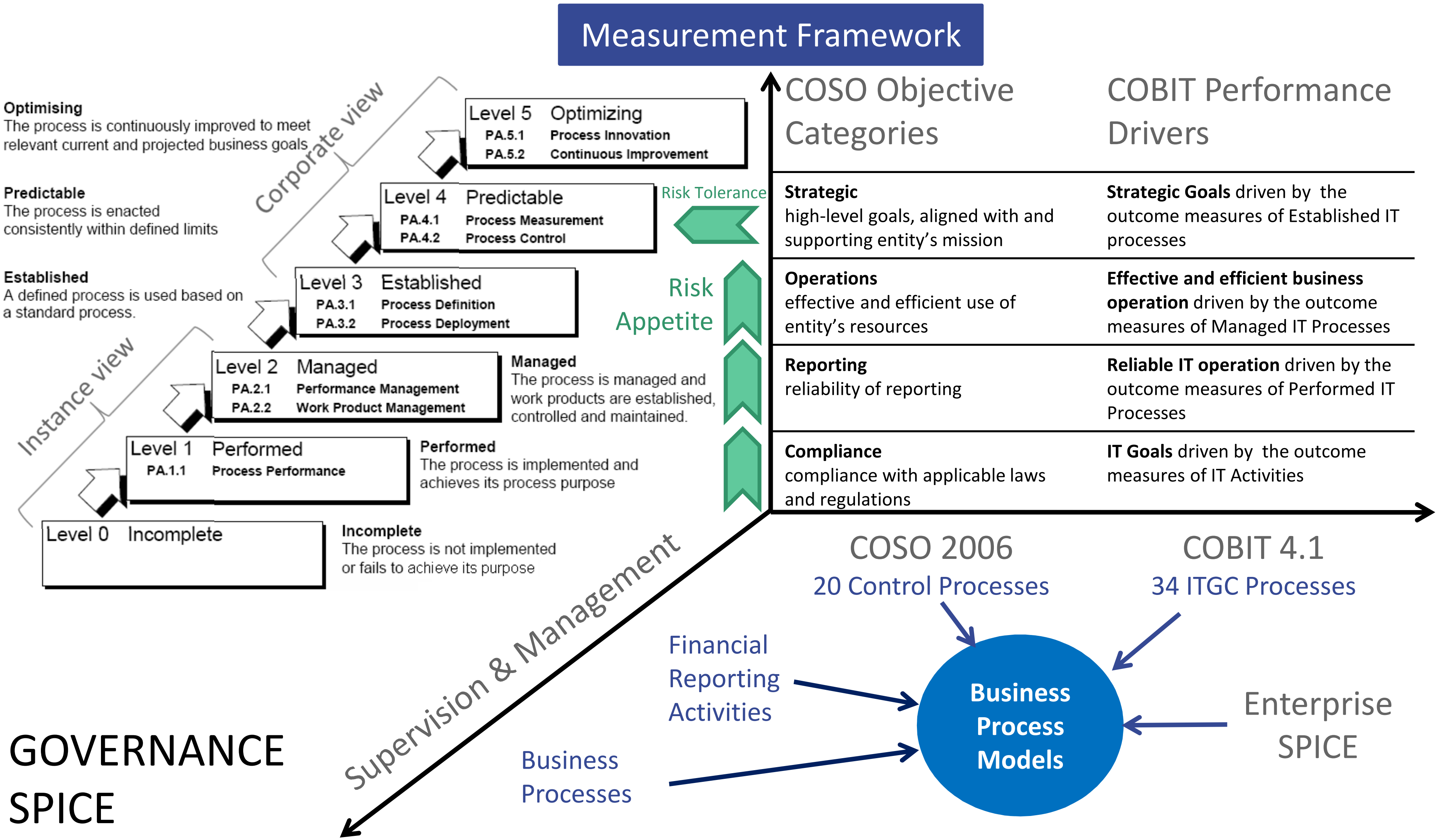
adding new concepts

- Control model updates (COBIT 2012, COSO 2013)
- ISO 31000 Risk Management

focusing on SMEs

- Improving management and audit skills
- Fostering better visibility on the local and global marketplaces

Governance SPICE: Capability Measures for Assurance and Improvement



Measurement Framework

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

Predictable
The process is enacted consistently within defined limits

Established
A defined process is used based on a standard process.

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

Performed
The process is implemented and achieves its process purpose

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

Corporate view
Instance view
Level 5 Optimizing
PA.5.1 Process Innovation
PA.5.2 Continuous Improvement
Level 4 Predictable
PA.4.1 Process Measurement
PA.4.2 Process Control
Level 3 Established
PA.3.1 Process Definition
PA.3.2 Process Deployment
Level 2 Managed
PA.2.1 Performance Management
PA.2.2 Work Product Management
Level 1 Performed
PA.1.1 Process Performance
Level 0 Incomplete
Risk Tolerance
Risk Appetite
Supervision & Management

COSO Objective Categories	COBIT Performance Drivers
Strategic high-level goals, aligned with and supporting entity's mission	**Strategic Goals** driven by the outcome measures of Established IT processes
Operations effective and efficient use of entity's resources	**Effective and efficient business operation** driven by the outcome measures of Managed IT Processes
Reporting reliability of reporting	**Reliable IT operation** driven by the outcome measures of Performed IT Processes
Compliance compliance with applicable laws and regulations	**IT Goals** driven by the outcome measures of IT Activities

COSO 2006
20 Control Processes

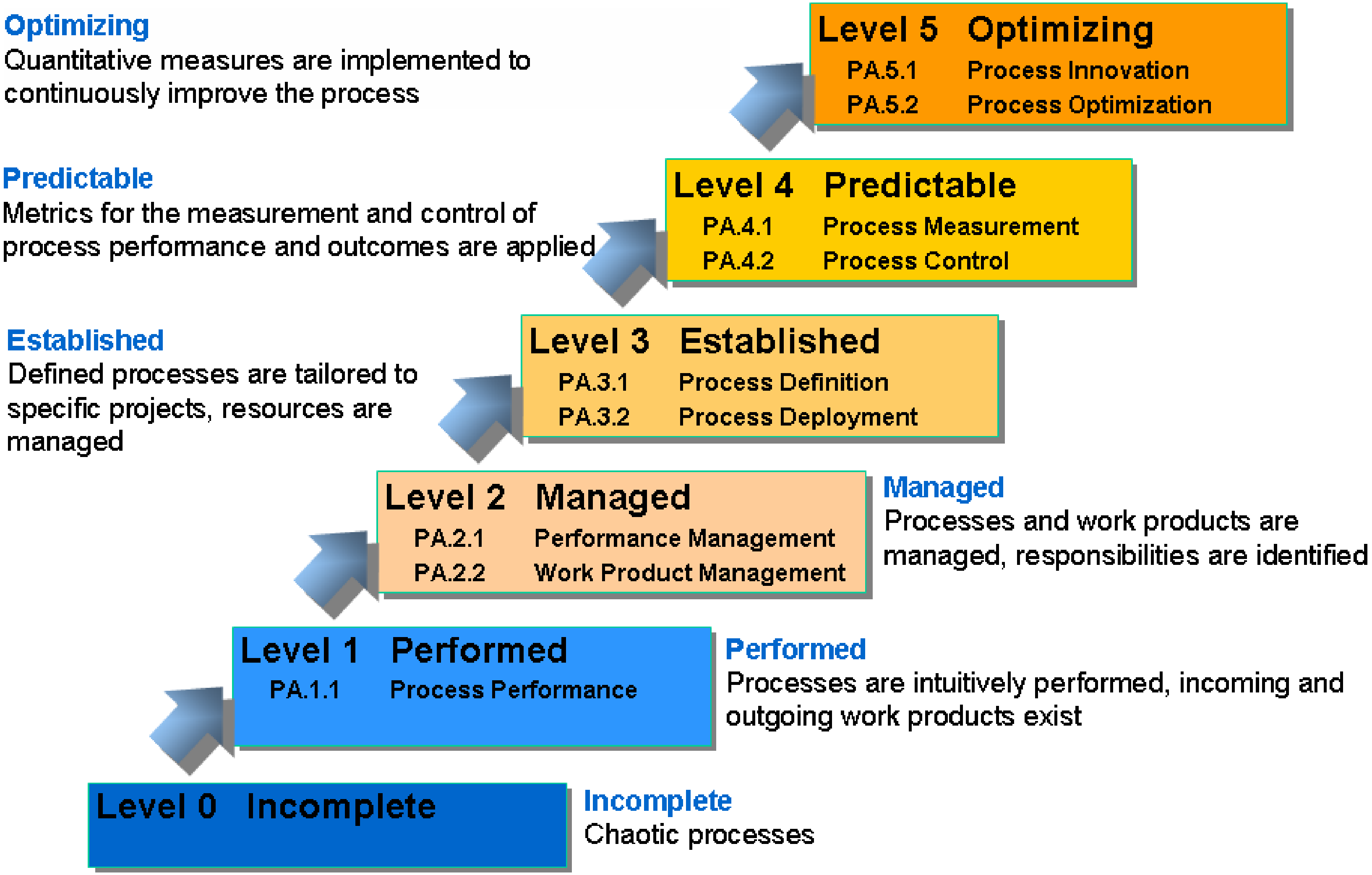
COBIT 4.1
34 ITGC Processes

GOVERNANCE SPICE

Linking Governance Objectives to Process Capability

- Governance (COSO) objectives:
  - Compliance with applicable laws and regulations
  - Reliable reporting
  - Effective and efficient operations
  - Aligned with strategy
- Process capability (ISO/IEC 15504 – ”SPICE”) goals:
  - Achieving purpose
  - Managing performance
  - Applying entity level ”standards”
  - Control by linking performance metrics to business objectives

Process Capability Levels



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

Optimizing
Quantitative measures are implemented to continuously improve the process

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

Predictable
Metrics for the measurement and control of process performance and outcomes are applied

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

Established
Defined processes are tailored to specific projects, resources are managed

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

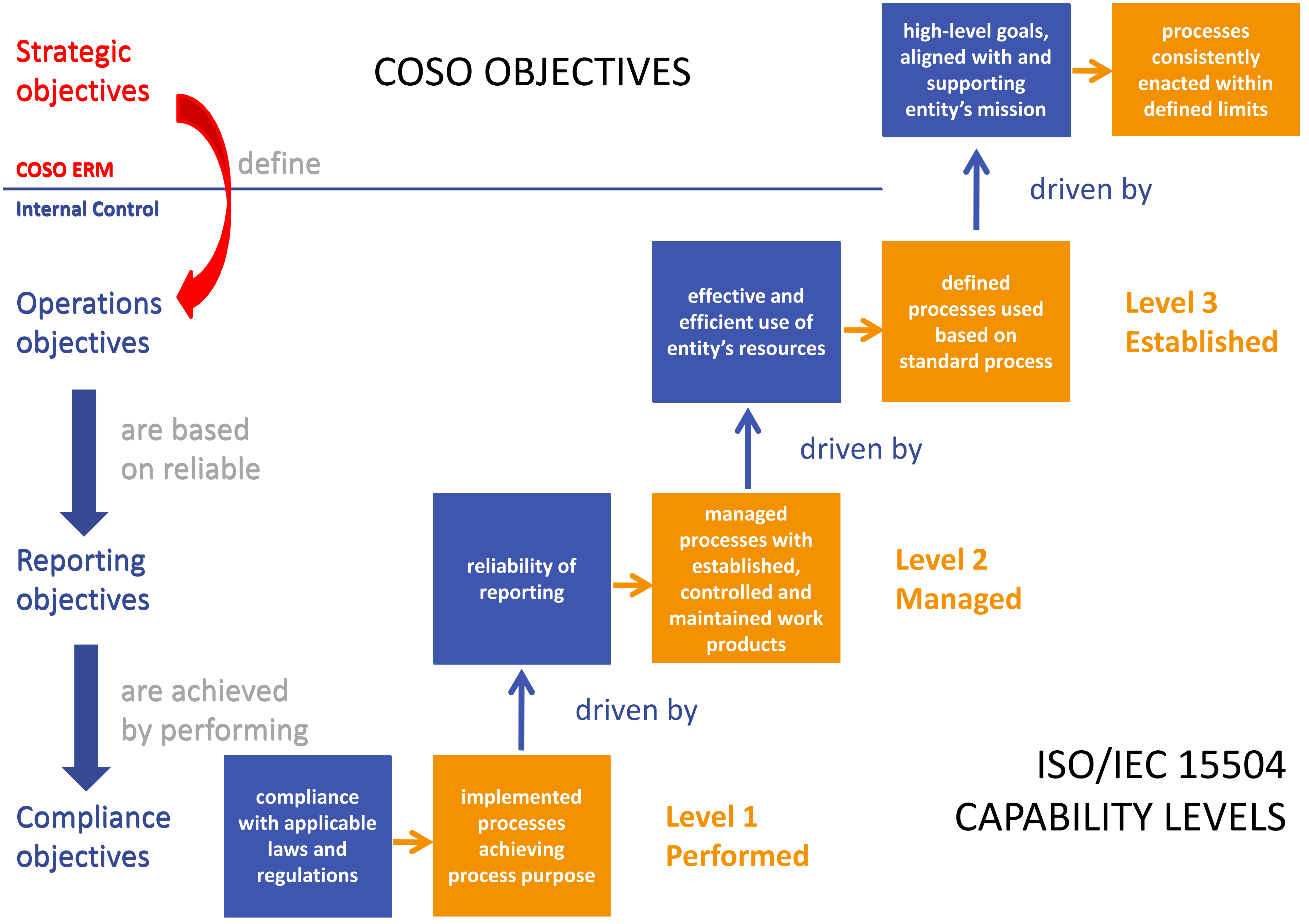
Managed
Processes and work products are managed, responsibilities are identified

Level 1 Performed
PA.1.1 Process Performance

Performed
Processes are intuitively performed, incoming and outgoing work products exist

Level 0 Incomplete

Incomplete
Chaotic processes



COSO OBJECTIVES

Strategic objectives

define

COSO ERM

Internal Control

Operations objectives

are based on reliable

Reporting objectives

are achieved by performing

Compliance objectives

compliance with applicable laws and regulations

implemented processes achieving process purpose

Level 1 Performed

driven by

reliability of reporting

managed processes with established, controlled and maintained work products

Level 2 Managed

driven by

effective and efficient use of entity's resources

defined processes used based on standard process

Level 3 Established

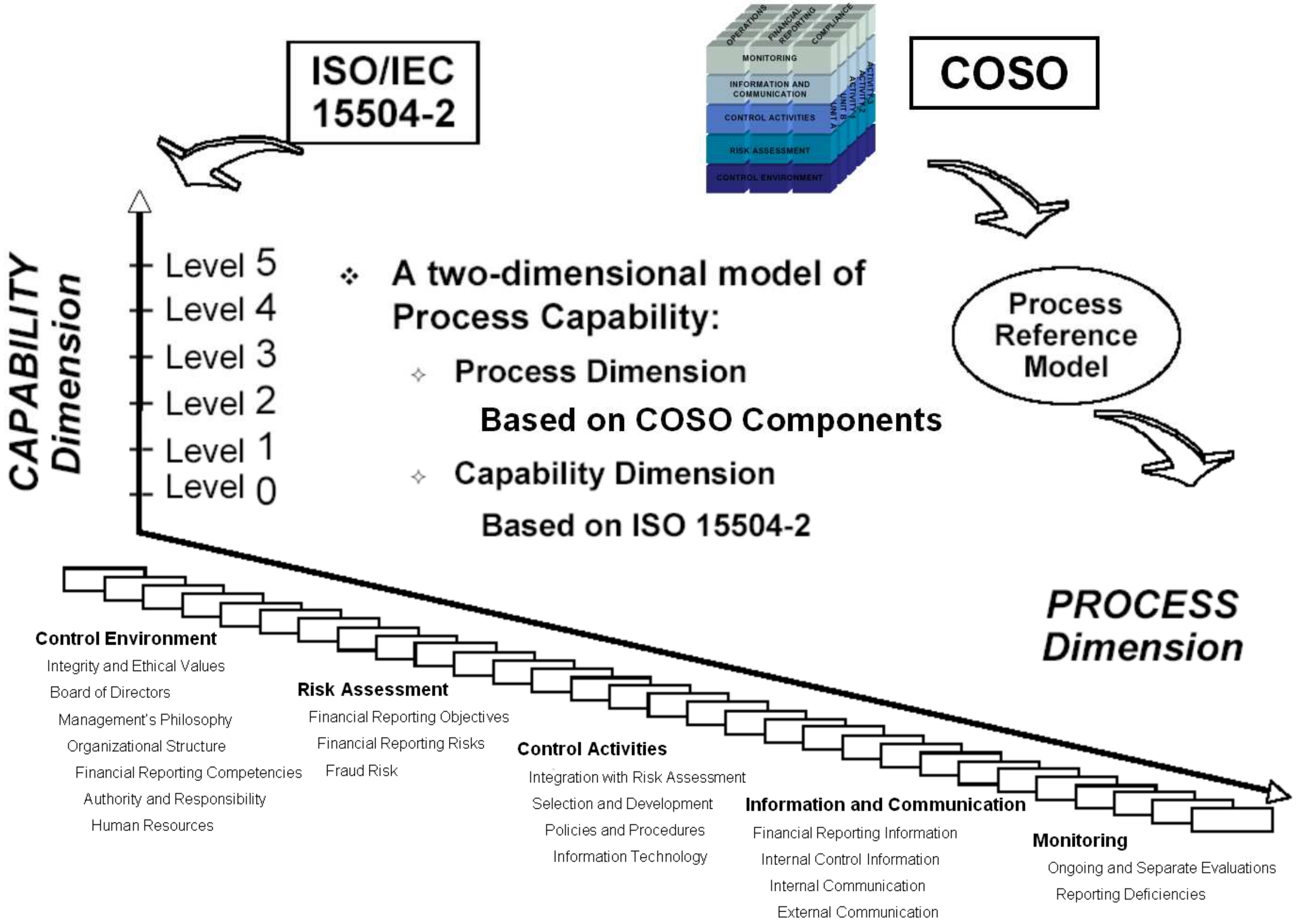
driven by

high-level goals, aligned with and supporting entity's mission

processes consistently enacted within defined limits

ISO/IEC 15504 CAPABILITY LEVELS

COSO Components as Process Dimension



- A two-dimensional model of Process Capability:
  - Process Dimension

    Based on COSO Components
  - Capability Dimension

    Based on ISO 15504-2

Control Environment
Integrity and Ethical Values
Board of Directors
Management's Philosophy
Organizational Structure
Financial Reporting Competencies
Authority and Responsibility
Human Resources

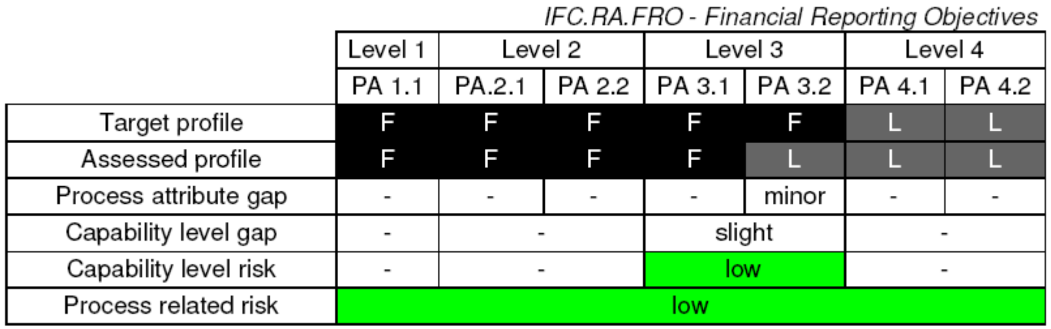
Risk Assessment
Financial Reporting Objectives
Financial Reporting Risks
Fraud Risk

Control Activities
Integration with Risk Assessment
Selection and Development
Policies and Procedures
Information Technology

Information and Communication
Financial Reporting Information
Internal Control Information
Internal Communication
External Communication

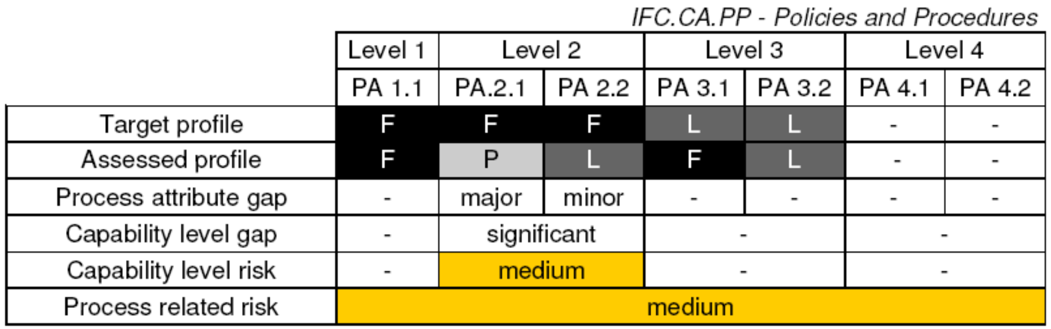
Monitoring
Ongoing and Separate Evaluations
Reporting Deficiencies

ISO/IEC 15504 based Control Risk Assessment



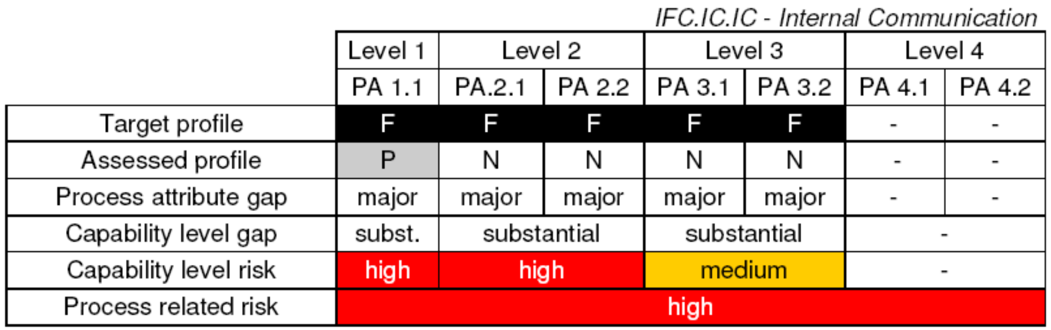
IFC.RA.FRO - Financial Reporting Objectives

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	F	F	L	L
Assessed profile	F	F	F	F	L	L	L
Process attribute gap	-	-	-	-	minor	-	-
Capability level gap	-	-		slight		-	
Capability level risk	-	-		low		-	
Process related risk	low						



IFC.CA.PP - Policies and Procedures

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	L	L	-	-
Assessed profile	F	P	L	F	L	-	-
Process attribute gap	-	major	minor	-	-	-	-
Capability level gap	-	significant		-		-	
Capability level risk	-	medium		-		-	
Process related risk	medium						



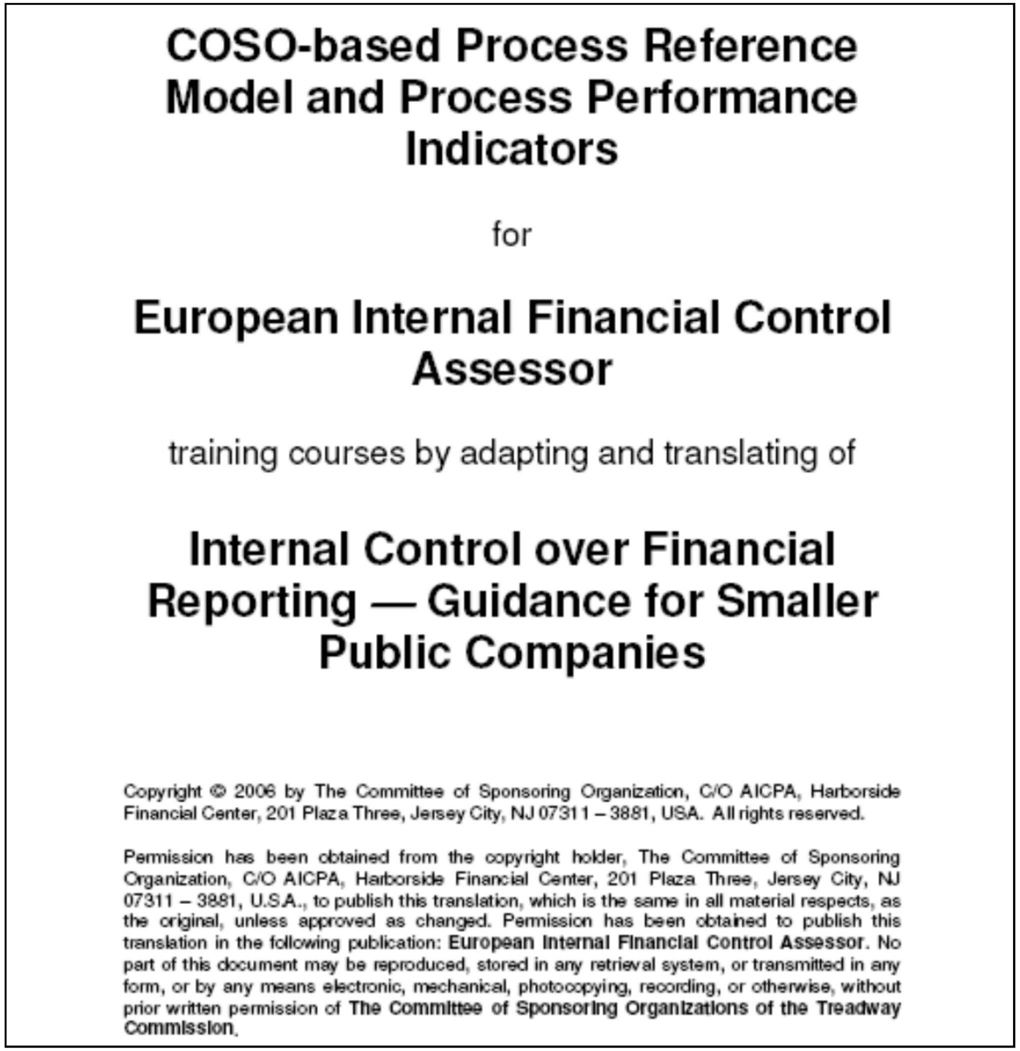
IFC.IC.IC - Internal Communication

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	F	F	-	-
Assessed profile	P	N	N	N	N	-	-
Process attribute gap	major	major	major	major	major	-	-
Capability level gap	subst.	substantial		substantial		-	
Capability level risk	high	high		medium		-	
Process related risk	high						

Internal Control over Financial Reporting - Guidance for Smaller Public Companies

Volume I : Executive Summary

Using COSO 2006 Guidance for PRM and Level 1 Indicators



COSO-based Process Reference Model and Process Performance Indicators

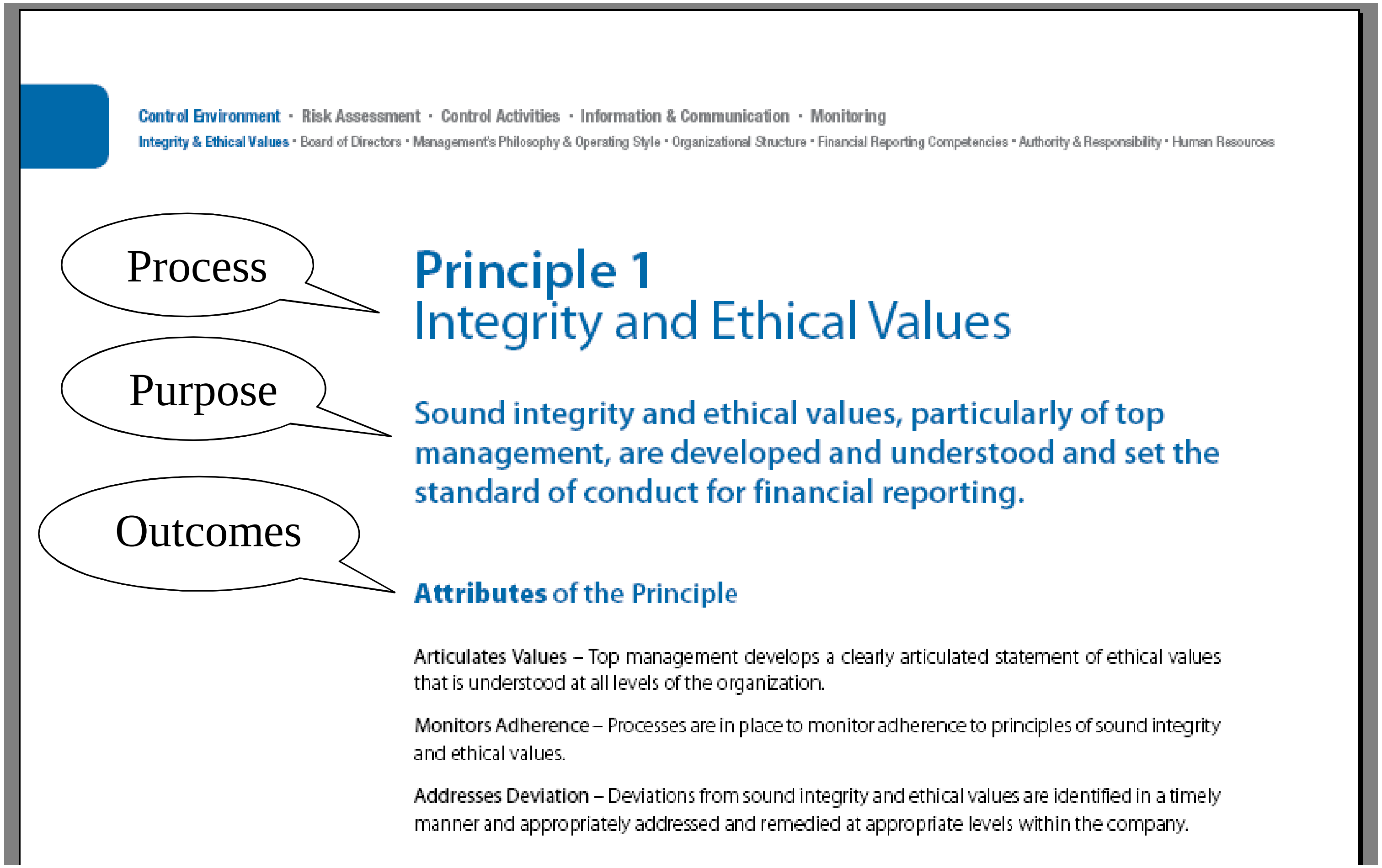
for

European Internal Financial Control Assessor

training courses by adapting and translating of

Internal Control over Financial Reporting — Guidance for Smaller Public Companies

COSO 2006 Guidance – ISO/IEC 15504 PRM



Process
Purpose
Outcomes

Control Environment · Risk Assessment · Control Activities · Information & Communication · Monitoring

Integrity & Ethical Values · Board of Directors · Management's Philosophy & Operating Style · Organizational Structure · Financial Reporting Competencies · Authority & Responsibility · Human Resources

Principle 1
Integrity and Ethical Values

Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.

Attributes of the Principle

Articulates Values – Top management develops a clearly articulated statement of ethical values that is understood at all levels of the organization.

Monitors Adherence – Processes are in place to monitor adherence to principles of sound integrity and ethical values.

Addresses Deviation – Deviations from sound integrity and ethical values are identified in a timely manner and appropriately addressed and remedied at appropriate levels within the company.

COSO 2006 Guidance – ISO/IEC 15504 PRM

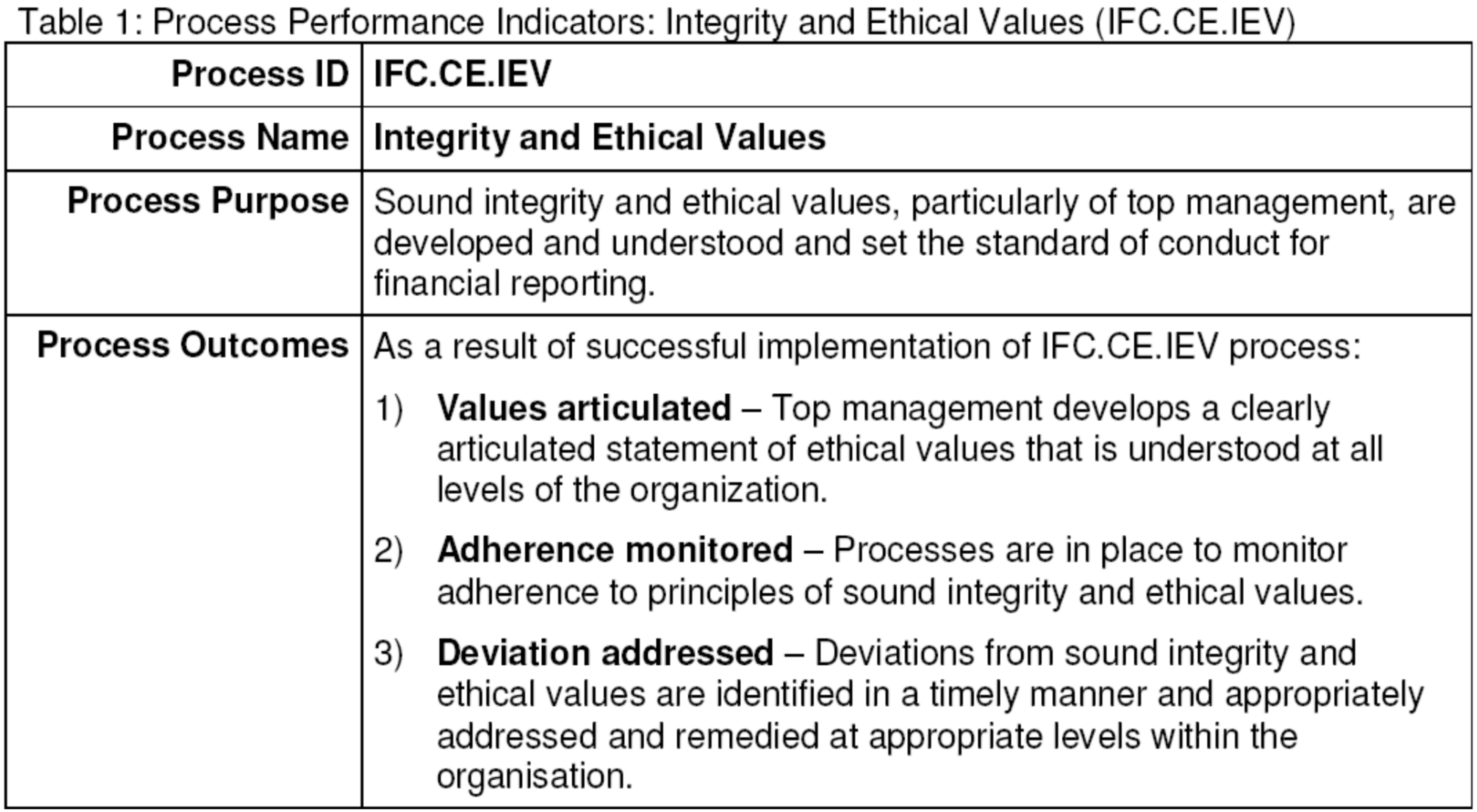
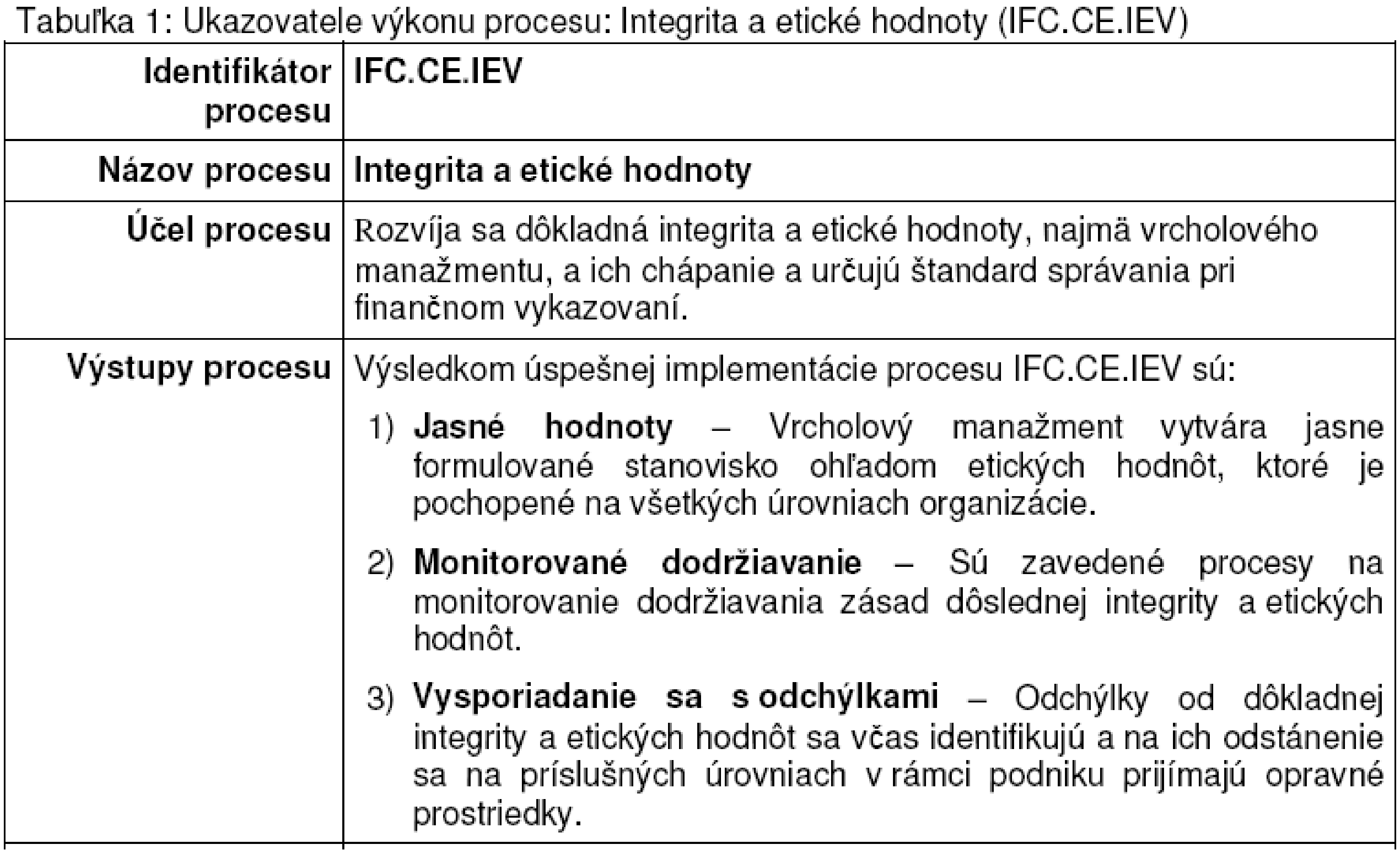


Table 1: Process Performance Indicators: Integrity and Ethical Values (IFC.CE.IEV)

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.

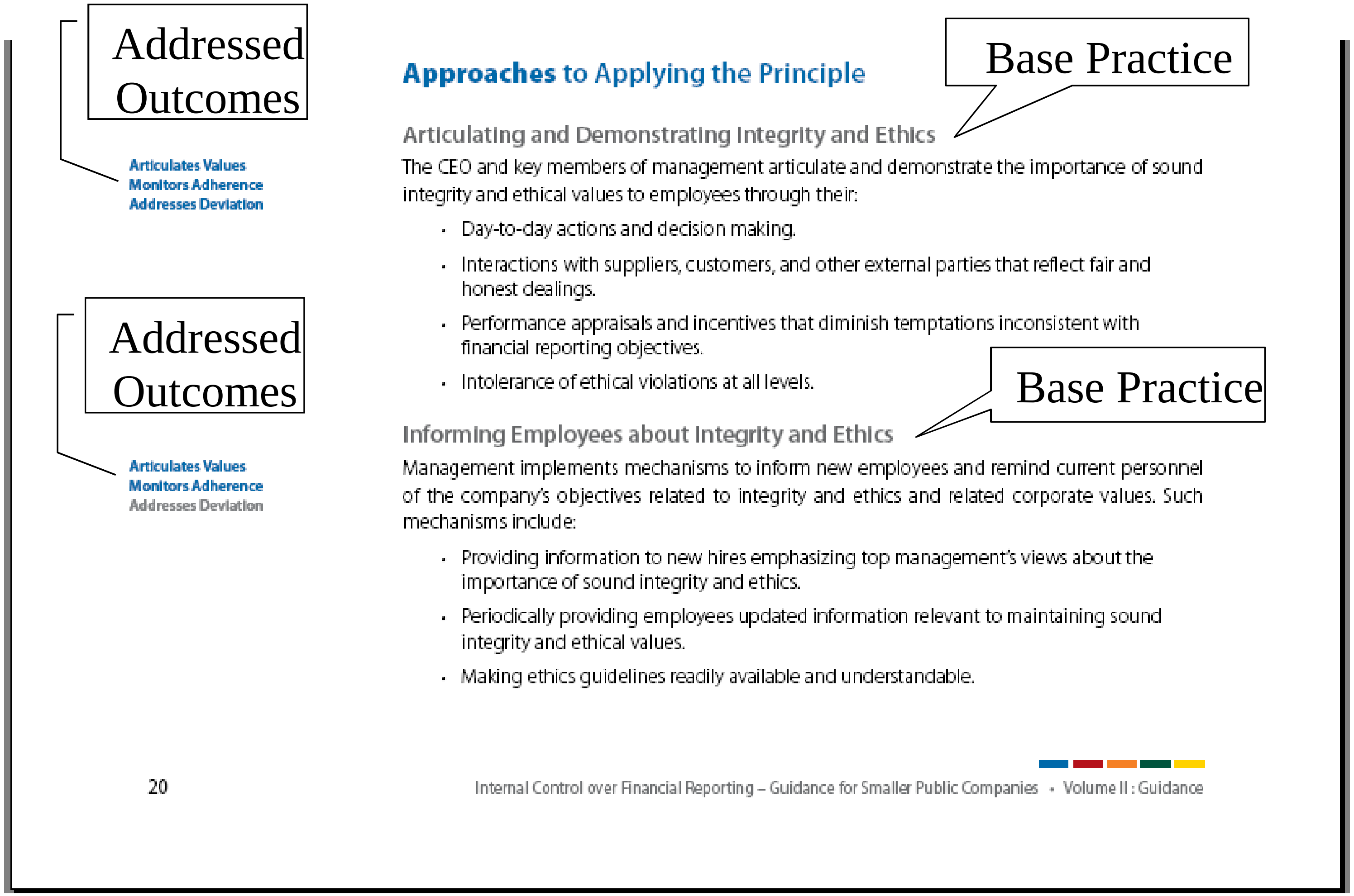
COSO 2006 Guidance – ISO/IEC 15504 PRM



Tabuľka 1: Ukazovatele výkonu procesu: Integrita a etické hodnoty (IFC.CE.IEV)

Identifikátor procesu	**IFC.CE.IEV**
Názov procesu	**Integrita a etické hodnoty**
Účel procesu	Rozvíja sa dôkladná integrita a etické hodnoty, najmä vrcholového manažmentu, a ich chápanie a určujú štandard správania pri finančnom vykazovaní.
Výstupy procesu	Výsledkom úspešnej implementácie procesu IFC.CE.IEV sú: 1) **Jasné hodnoty** – Vrcholový manažment vytvára jasne formulované stanovisko ohľadom etických hodnôt, ktoré je pochopené na všetkých úrovniach organizácie. 2) **Monitorované dodržiavanie** – Sú zavedené procesy na monitorovanie dodržiavania zásad dôslednej integrity a etických hodnôt. 3) **Vysporiadanie sa s odchýlkami** – Odchýlky od dôkladnej integrity a etických hodnôt sa včas identifikujú a na ich odstánenie sa na príslušných úrovniach v rámci podniku prijímajú opravné prostriedky.

COSO 2006 Guidance – Level 1 Indicators



Addressed Outcomes

Articulates Values
Monitors Adherence
Addresses Deviation

Base Practice

Approaches to Applying the Principle

Articulating and Demonstrating Integrity and Ethics

The CEO and key members of management articulate and demonstrate the importance of sound integrity and ethical values to employees 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.

Addressed Outcomes

Articulates Values
Monitors Adherence
Addresses Deviation

Base Practice

Informing Employees about Integrity and Ethics

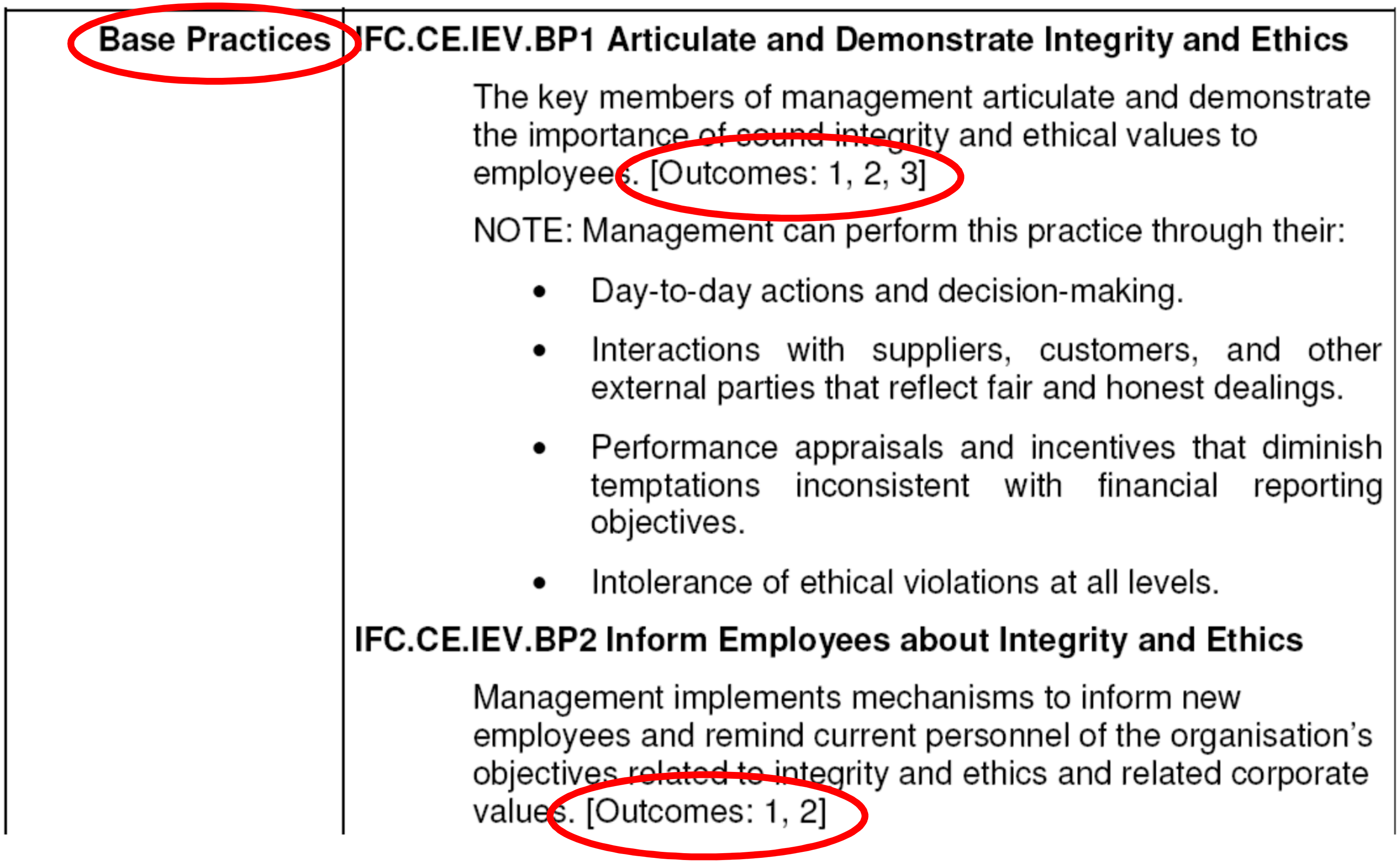
Management implements mechanisms to inform new employees and remind current personnel of the company's objectives related to integrity and ethics and related corporate values. Such mechanisms include:

- Providing information to new hires emphasizing top management's views about the importance of sound integrity and ethics.
- Periodically providing employees updated information relevant to maintaining sound integrity and ethical values.
- Making ethics guidelines readily available and understandable.

20

Internal Control over Financial Reporting – Guidance for Smaller Public Companies • Volume II : Guidance

COSO 2006 Guidance – Level 1 Indicators



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]

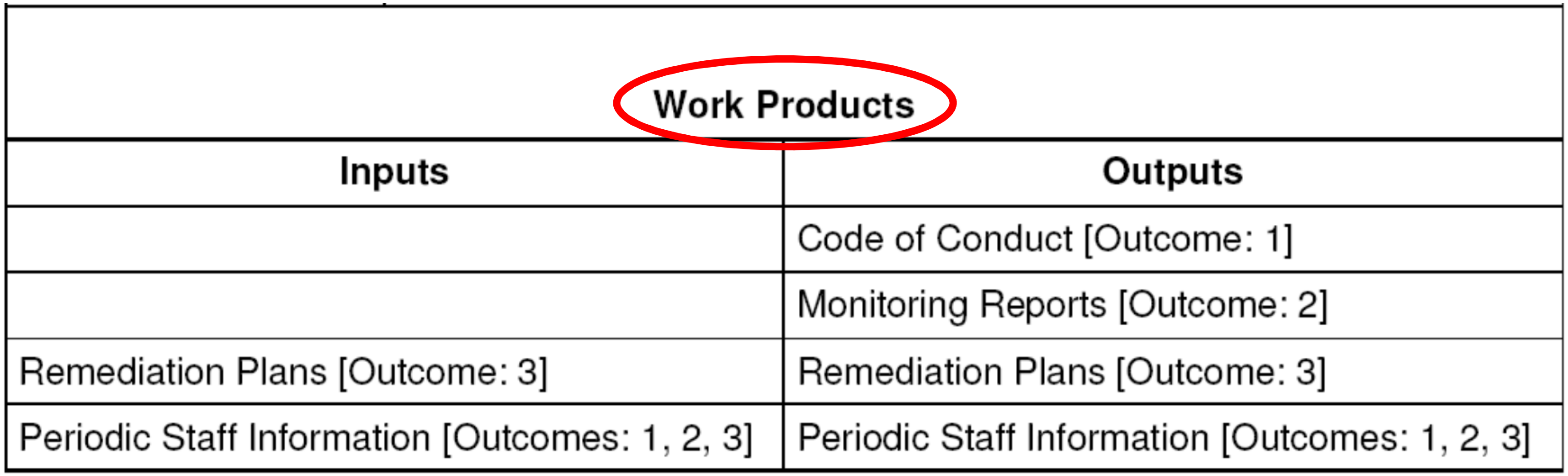
NOTE: Management can perform this practice through their:

- 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

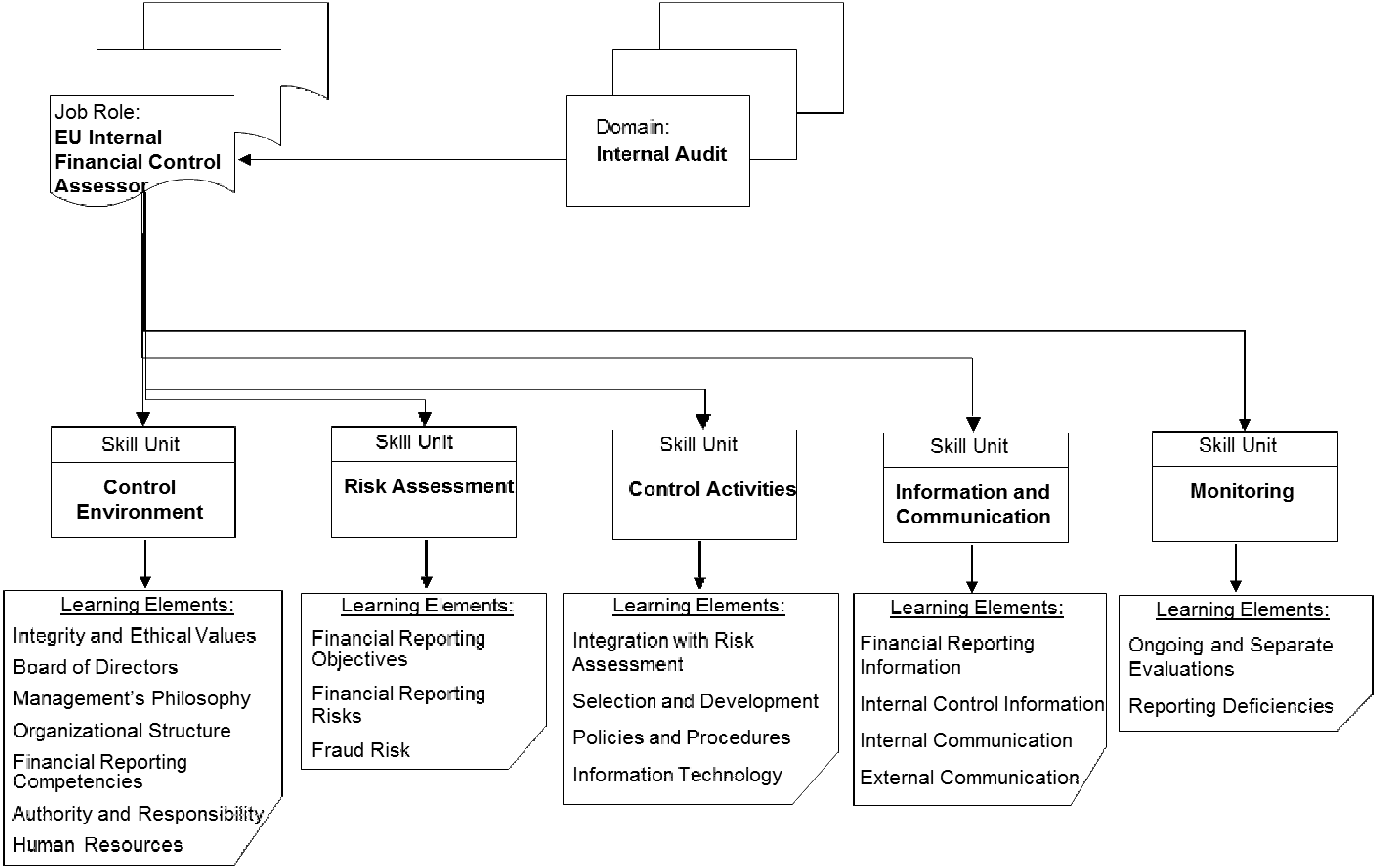
Management implements mechanisms to inform new employees and remind current personnel of the organisation's objectives related to integrity and ethics and related corporate values. [Outcomes: 1, 2]

COSO 2006 Guidance – Level 1 Indicators



Work Products	
Inputs	**Outputs**
	Code of Conduct [Outcome: 1]
	Monitoring Reports [Outcome: 2]
Remediation Plans [Outcome: 3]	Remediation Plans [Outcome: 3]
Periodic Staff Information [Outcomes: 1, 2, 3]	Periodic Staff Information [Outcomes: 1, 2, 3]

Internal Financial Control Assessor Skillcard



Job Role: **EU Internal Financial Control Assessor**

Domain: **Internal Audit**

Skill Unit **Control Environment**

Learning Elements:
- Integrity and Ethical Values
- Board of Directors
- Management's Philosophy
- Organizational Structure
- Financial Reporting Competencies
- Authority and Responsibility
- Human Resources

Skill Unit **Risk Assessment**

Learning Elements:
- Financial Reporting Objectives
- Financial Reporting Risks
- Fraud Risk

Skill Unit **Control Activities**

Learning Elements:
- Integration with Risk Assessment
- Selection and Development
- Policies and Procedures
- Information Technology

Skill Unit **Information and Communication**

Learning Elements:
- Financial Reporting Information
- Internal Control Information
- Internal Communication
- External Communication

Skill Unit **Monitoring**

Learning Elements:
- Ongoing and Separate Evaluations
- Reporting Deficiencies

Internal Financial Control Assessment

- The methodology and the related training program were developed by the ”IA-Manager” pilot LdV project (2005-2007)
- Based on ISO/IEC 15504 (SPICE) and the COSO 2006 Guidance (as process reference model)
- International partnership (HU, IRL, ES, RO, BE)
- Recognized internationally by professional bodies, like the COSO, the Institute of Internal Auditors, the European Court of Auditors, etc.
- Pilot trainings and exams from 2007
- Revision by the MONTIFIC project (2008-2010)

The MONTIFIC project

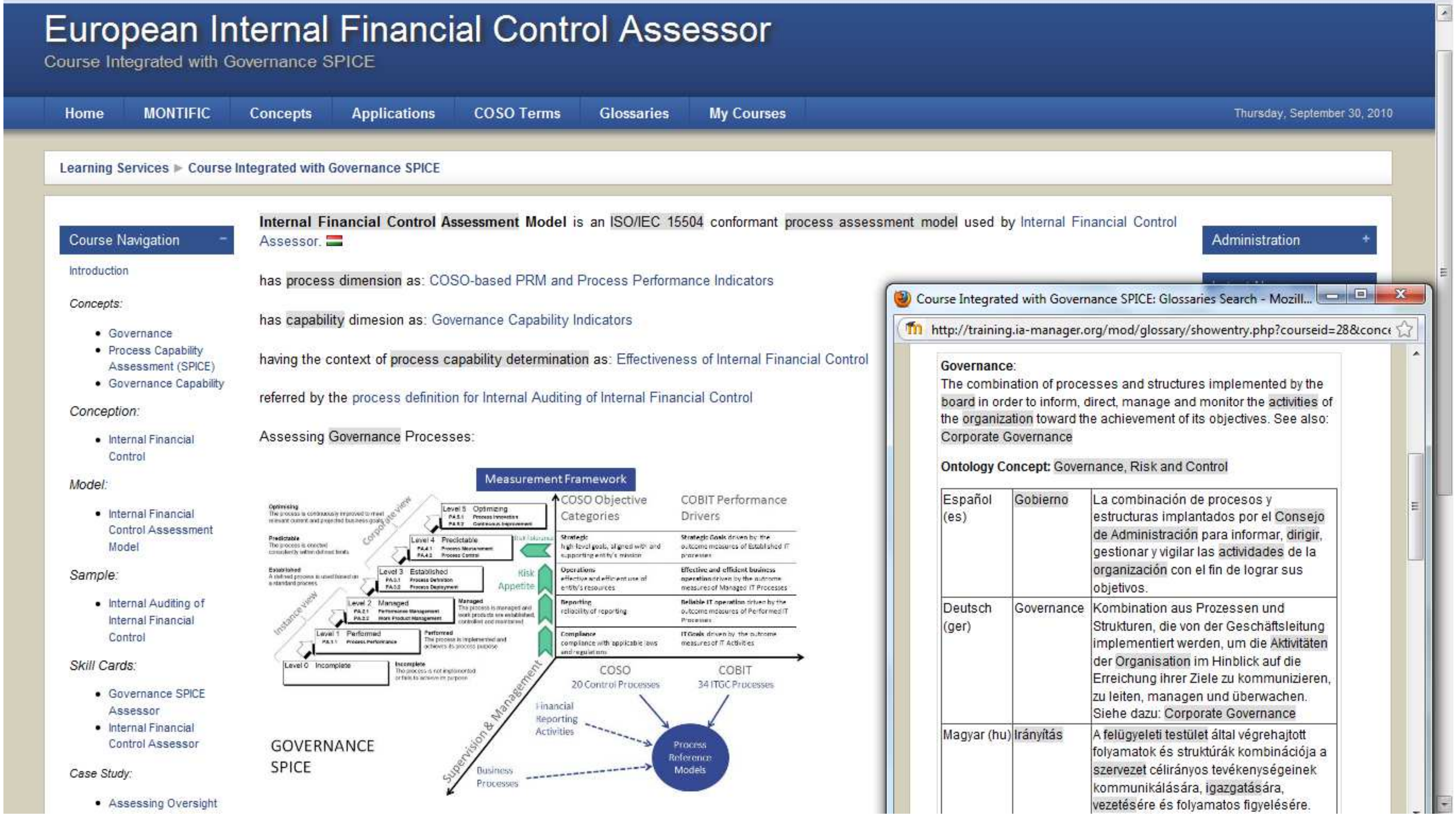
Implementing an ontology-driven multilingual terminology database for achieving the following specific objectives:

- Facilitating local training providers (trainers) and trainees in using their own languages based on multilingual ontology,
- Involving European Certification and Qualification Association for providing online exams and certification programme in more local languages,
- Supporting certification holders (assessors) and wider potential user communities by utilizing common knowledge (terminology) in different countries and working environments,
- Further developing multilingual e-content tools based on the terminology and ontology interoperability framework (online learning, certification and assessment portals).

The MONTIFIC Book

- Possibilities, Responsibilities and International Trends of Auditing in Autumn 2010
- Governance Practices of Supporting Innovation
- Governance Capability Assessment: Using ISO/IEC 15504 for Internal Financial Controls and IT Management
- Added Value of a Multilingual Internal Financial Control Ontology for Accounting Profession
- Terminology and Ontology Interoperability Model for Internal Financial Control Assessor Learning Environment
- Ontology-based Multilingual Access to Financial Reports for Sharing Business Knowledge across Europe
- Integrated COSO SPICE Assessments
- Human Resources Based Improvement Strategies – the Learning Factor

Learning ontology and multilingual glossary



European Internal Financial Control Assessor
Course Integrated with Governance SPICE

Introduction

Concepts:

- Governance
- Process Capability Assessment (SPICE)
- Governance Capability

Conception:

- Internal Financial Control

Model:

- Internal Financial Control Assessment Model

Sample:

- Internal Auditing of Internal Financial Control

Skill Cards:

- Governance SPICE Assessor
- Internal Financial Control Assessor

Case Study:

- Assessing Oversight

Internal Financial Control Assessment Model is an ISO/IEC 15504 conformant process assessment model used by Internal Financial Control Assessor.

has process dimension as: COSO-based PRM and Process Performance Indicators

has capability dimesion as: Governance Capability Indicators

having the context of process capability determination as: Effectiveness of Internal Financial Control

referred by the process definition for Internal Auditing of Internal Financial Control

Assessing Governance Processes:

Measurement Framework
Optimising
The process is continuously improved to meet relevant current and projected business goals
Predictable
The process is enacted consistently within defined limits
Established
A defined process is used based on a standard process
Corporate view
Instance view
Level 5 Optimizing
PA.5.1 Process Innovation
PA.5.2 Continuous Improvement
Level 4 Predictable
PA.4.1 Process Measurement
PA.4.2 Process Control
Level 3 Established
PA.3.1 Process Definition
PA.3.2 Process Deployment
Level 2 Managed
PA.2.1 Performance Management
PA.2.2 Work Product Management
Level 1 Performed
PA.1.1 Process Performance
Level 0 Incomplete
Managed
The process is managed and work products are established, controlled and maintained
Performed
The process is implemented and achieves its process purpose
Incomplete
The process is not implemented or fails to achieve its purpose
Risk Tolerance
Risk Appetite
COSO Objective Categories
COBIT Performance Drivers
Strategic
high-level goals, aligned with and supporting entity's mission
Strategic Goals driven by the outcome measures of Established IT processes
Operations
effective and efficient use of entity's resources
Effective and efficient business operation driven by the outcome measures of Managed IT Processes
Reporting
reliability of reporting
Reliable IT operation driven by the outcome measures of Performed IT Processes
Compliance
compliance with applicable laws and regulations
IT Goals driven by the outcome measures of IT Activities
COSO
20 Control Processes
COBIT
34 ITGC Processes
Supervision & Management
Financial Reporting Activities
Business Processes
Process Reference Models
GOVERNANCE
SPICE

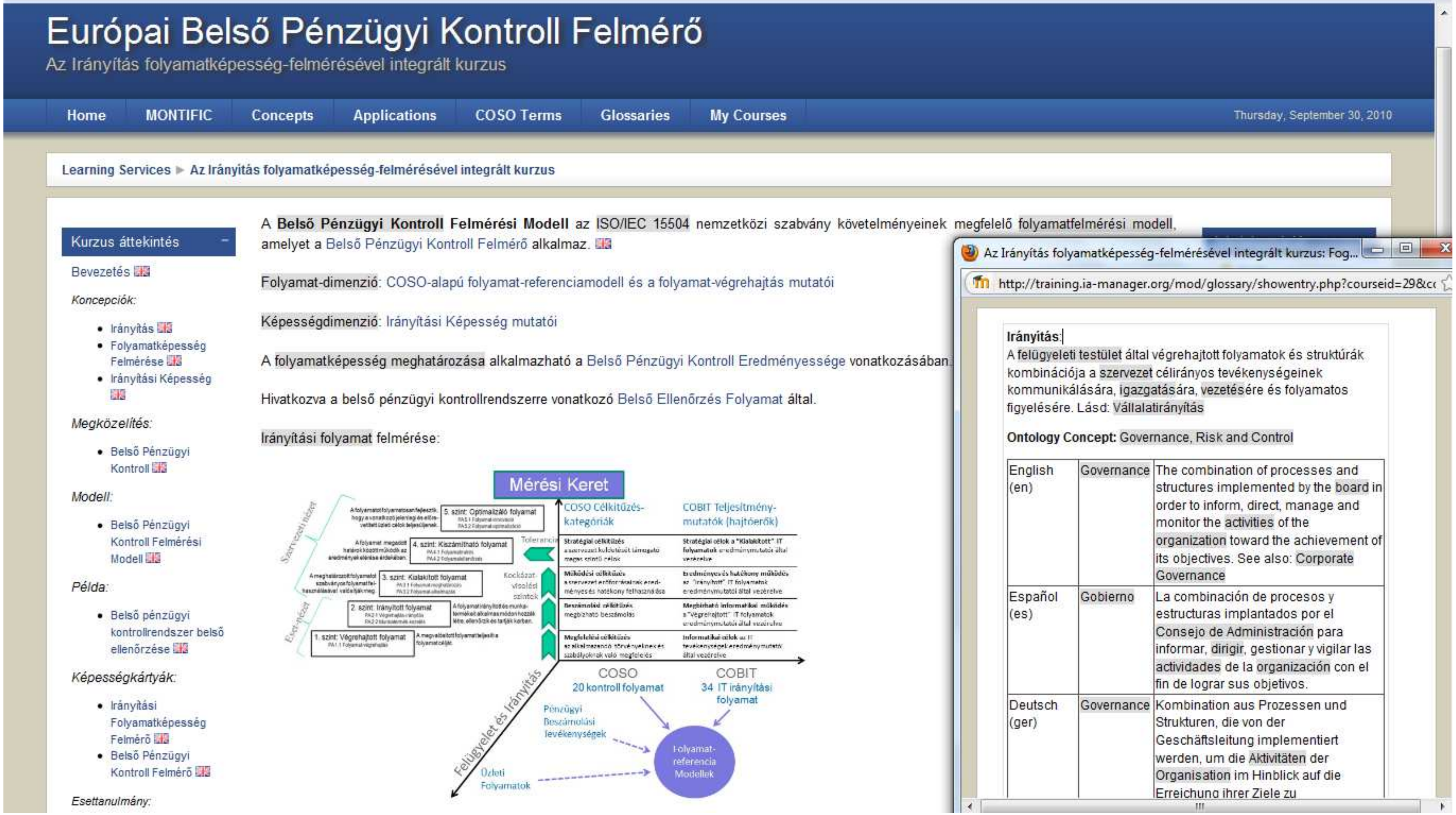
Course Integrated with Governance SPICE: Glossaries Search - Mozill...
http://training.ia-manager.org/mod/glossary/showentry.php?courseid=28&conce

Governance:
The combination of processes and structures implemented by the board in order to inform, direct, manage and monitor the activities of the organization toward the achievement of its objectives. See also: Corporate Governance

Ontology Concept: Governance, Risk and Control

Español (es)	Gobierno	La combinación de procesos y estructuras implantados por el Consejo de Administración para informar, dirigir, gestionar y vigilar las actividades de la organización con el fin de lograr sus objetivos.
Deutsch (ger)	Governance	Kombination aus Prozessen und Strukturen, die von der Geschäftsleitung implementiert werden, um die Aktivitäten der Organisation im Hinblick auf die Erreichung ihrer Ziele zu kommunizieren, zu leiten, managen und überwachen. Siehe dazu: Corporate Governance
Magyar (hu)	Irányítás	A felügyeleti testület által végrehajtott folyamatok és struktúrák kombinációja a szervezet célirányos tevékenységeinek kommunikálására, igazgatására, vezetésére és folyamatos figyelésére.

Learning ontology and multilingual glossary (HU)



Európai Belső Pénzügyi Kontroll Felmérő
Az Irányítás folyamatképesség-felmérésével integrált kurzus
Home
MONTIFIC
Concepts
Applications
COSO Terms
Glossaries
My Courses
Thursday, September 30, 2010
Learning Services ▶ Az Irányítás folyamatképesség-felmérésével integrált kurzus
Kurzus áttekintés

Bevezetés

Koncepciók:

- Irányítás
- Folyamatképesség Felmérése
- Irányítási Képesség

Megközelítés:

- Belső Pénzügyi Kontroll

Modell:

- Belső Pénzügyi Kontroll Felmérési Modell

Példa:

- Belső pénzügyi kontrollrendszer belső ellenőrzése

Képességkártyák:

- Irányítási Folyamatképesség Felmérő
- Belső Pénzügyi Kontroll Felmérő

Esettanulmány:

A **Belső Pénzügyi Kontroll Felmérési Modell** az ISO/IEC 15504 nemzetközi szabvány követelményeinek megfelelő folyamatfelmérési modell, amelyet a Belső Pénzügyi Kontroll Felmérő alkalmaz.

Folyamat-dimenzió: COSO-alapú folyamat-referenciamodell és a folyamat-végrehajtás mutatói

Képességdimenzió: Irányítási Képesség mutatói

A folyamatképesség meghatározása alkalmazható a Belső Pénzügyi Kontroll Eredményessége vonatkozásában.

Hivatkozva a belső pénzügyi kontrollrendszerre vonatkozó Belső Ellenőrzés Folyamat által.

Irányítási folyamat felmérése:

Mérési Keret
Szervezeti nézet
Eset-nézet
5. szint: Optimalizáló folyamat
4. szint: Kiszámítható folyamat
3. szint: Kialakított folyamat
2. szint: Irányított folyamat
1. szint: Végrehajtott folyamat
Tolerancia
Kockázat-viselési szintek
COSO Célkitűzés-kategóriák
COBIT Teljesítmény-mutatók (hajtóerők)
COSO
20 kontroll folyamat
COBIT
34 IT irányítási folyamat
Felügyelet és Irányítás
Pénzügyi Beszámolási Tevékenységek
Üzleti Folyamatok
Folyamat-referencia Modellek

Stratégiai célkitűzés: a szervezet küldetését támogató magas szintű célok — Stratégiai célok a "Kialakított" IT folyamatok eredménymutatói által vezérelve

Működési célkitűzés: a szervezet erőforrásainak eredményes és hatékony felhasználása — Eredményes és hatékony működés az "Irányított" IT folyamatok eredménymutatói által vezérelve

Beszámolási célkitűzés: megbízható beszámolás — Megbízható informatikai működés a "Végrehajtott" IT folyamatok eredménymutatói által vezérelve

Megfelelési célkitűzés: az alkalmazandó törvényeknek és szabályoknak való megfelelés — Informatikai célok az IT tevékenységek eredménymutatói által vezérelve

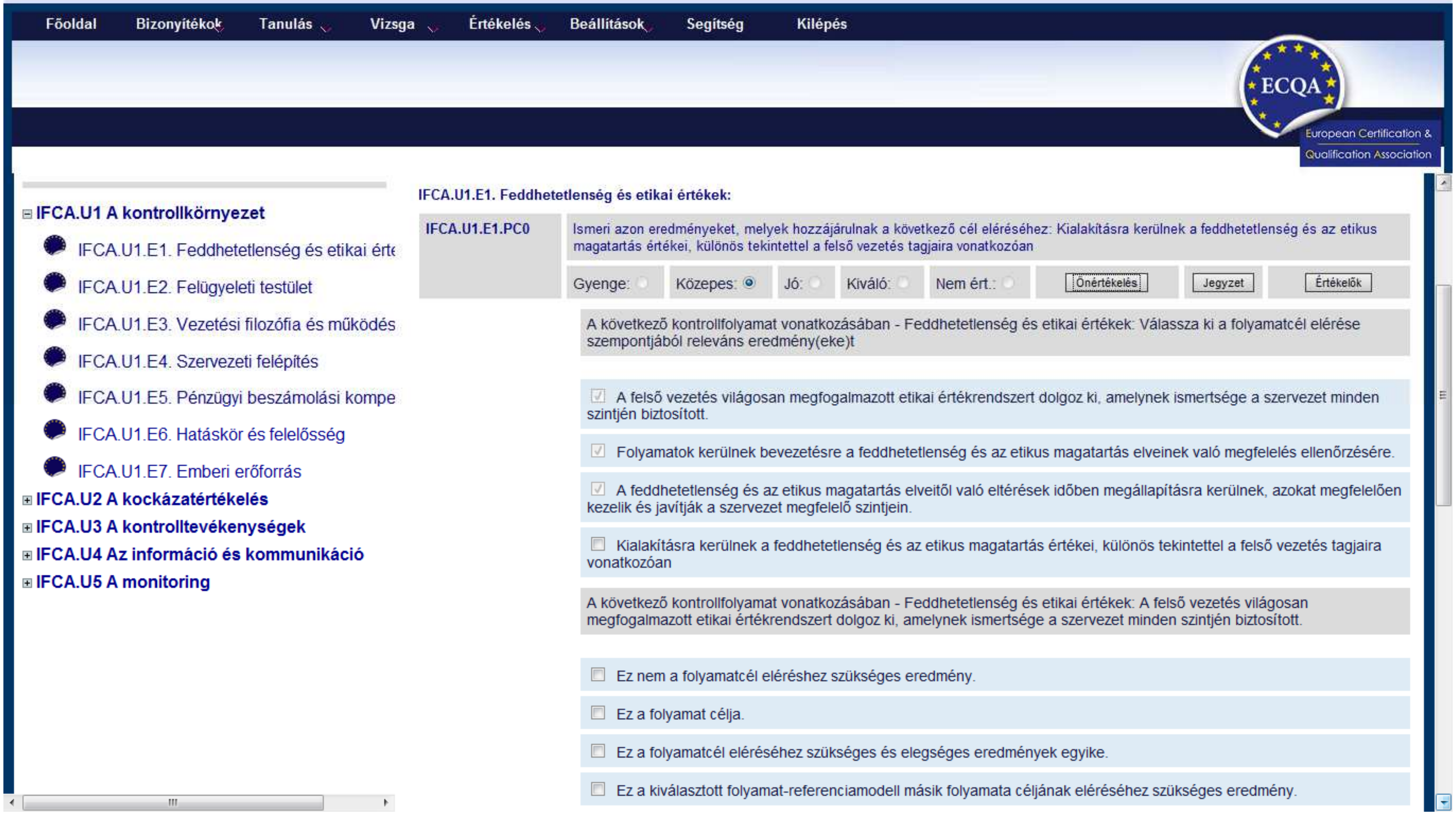
Az Irányítás folyamatképesség-felmérésével integrált kurzus: Fog...
http://training.ia-manager.org/mod/glossary/showentry.php?courseid=29&cc

Irányítás:
A felügyeleti testület által végrehajtott folyamatok és struktúrák kombinációja a szervezet célirányos tevékenységeinek kommunikálására, igazgatására, vezetésére és folyamatos figyelésére. Lásd: Vállalatirányítás

Ontology Concept: Governance, Risk and Control

English (en)	Governance	The combination of processes and structures implemented by the board in order to inform, direct, manage and monitor the activities of the organization toward the achievement of its objectives. See also: Corporate Governance
Español (es)	Gobierno	La combinación de procesos y estructuras implantados por el Consejo de Administración para informar, dirigir, gestionar y vigilar las actividades de la organización con el fin de lograr sus objetivos.
Deutsch (ger)	Governance	Kombination aus Prozessen und Strukturen, die von der Geschäftsleitung implementiert werden, um die Aktivitäten der Organisation im Hinblick auf die Erreichung ihrer Ziele zu

Multilingual Self-assessment & Exam Portal: www.ecqa.org



- ⊟ **IFCA.U1 A kontrollkörnyezet**
  - IFCA.U1.E1. Feddhetetlenség és etikai érte
  - IFCA.U1.E2. Felügyeleti testület
  - IFCA.U1.E3. Vezetési filozófia és működés
  - IFCA.U1.E4. Szervezeti felépítés
  - IFCA.U1.E5. Pénzügyi beszámolási kompe
  - IFCA.U1.E6. Hatáskör és felelősség
  - IFCA.U1.E7. Emberi erőforrás
- ⊞ **IFCA.U2 A kockázatértékelés**
- ⊞ **IFCA.U3 A kontrolltevékenységek**
- ⊞ **IFCA.U4 Az információ és kommunikáció**
- ⊞ **IFCA.U5 A monitoring**

IFCA.U1.E1. Feddhetetlenség és etikai értékek:

IFCA.U1.E1.PC0 Ismeri azon eredményeket, melyek hozzájárulnak a következő cél eléréséhez: Kialakításra kerülnek a feddhetetlenség és az etikus magatartás értékei, különös tekintettel a felső vezetés tagjaira vonatkozóan

Gyenge: ○ Közepes: ● Jó: ○ Kiváló: ○ Nem ért.: ○ [Önértékelés] [Jegyzet] [Értékelők]

A következő kontrollfolyamat vonatkozásában - Feddhetetlenség és etikai értékek: Válassza ki a folyamatcél elérése szempontjából releváns eredmény(eke)t

☑ A felső vezetés világosan megfogalmazott etikai értékrendszert dolgoz ki, amelynek ismertsége a szervezet minden szintjén biztosított.

☑ Folyamatok kerülnek bevezetésre a feddhetetlenség és az etikus magatartás elveinek való megfelelés ellenőrzésére.

☑ A feddhetetlenség és az etikus magatartás elveitől való eltérések időben megállapításra kerülnek, azokat megfelelően kezelik és javítják a szervezet megfelelő szintjein.

☐ Kialakításra kerülnek a feddhetetlenség és az etikus magatartás értékei, különös tekintettel a felső vezetés tagjaira vonatkozóan

A következő kontrollfolyamat vonatkozásában - Feddhetetlenség és etikai értékek: A felső vezetés világosan megfogalmazott etikai értékrendszert dolgoz ki, amelynek ismertsége a szervezet minden szintjén biztosított.

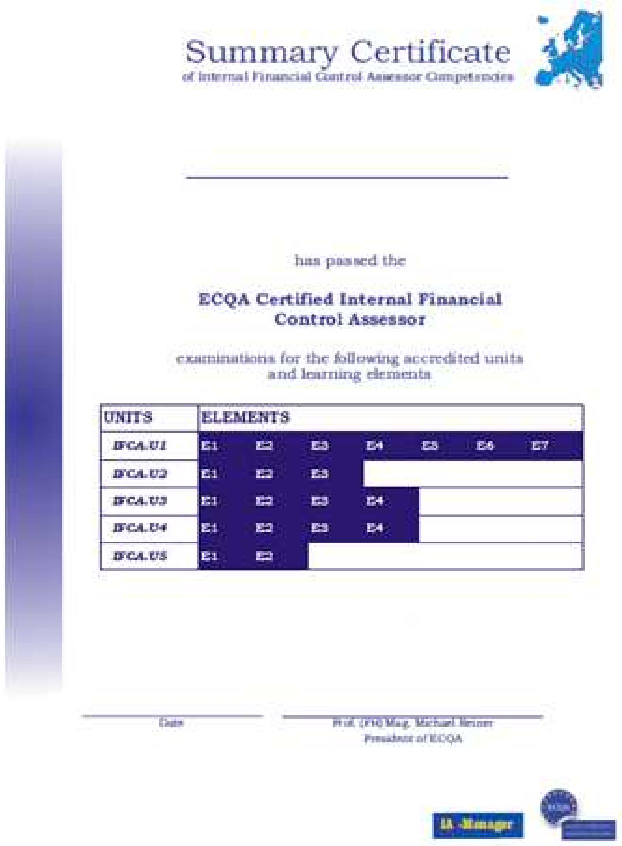
☐ Ez nem a folyamatcél eléréshez szükséges eredmény.

☐ Ez a folyamat célja.

☐ Ez a folyamatcél eléréséhez szükséges és elegséges eredmények egyike.

☐ Ez a kiválasztott folyamat-referenciamodell másik folyamata céljának eléréséhez szükséges eredmény.

ECQA certified
Internal Financial Control Assessor



Summary Certificate
of Internal Financial Control Assessor Competencies

has passed the

ECQA Certified Internal Financial Control Assessor

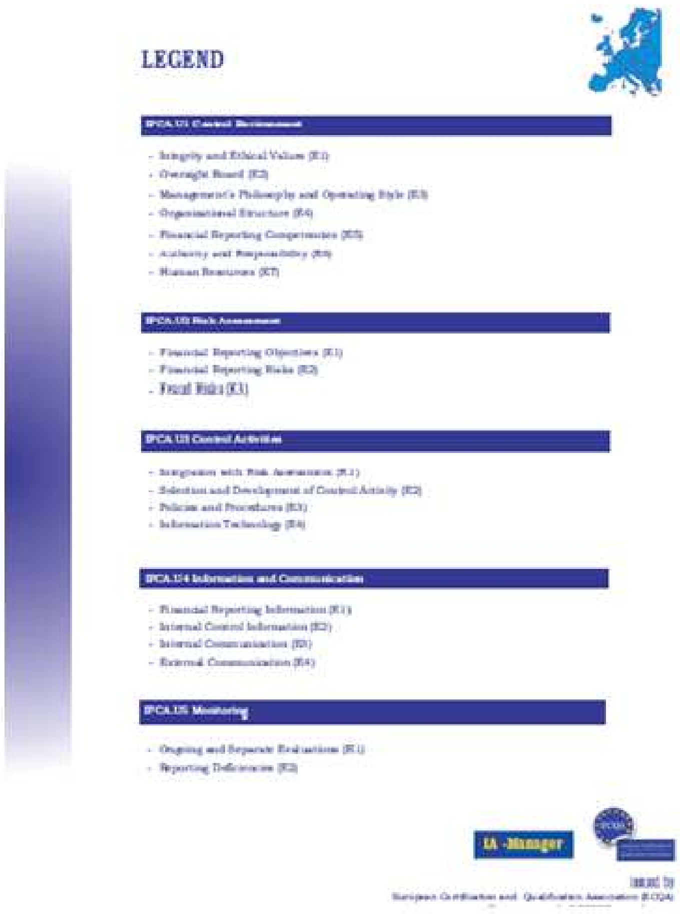
examinations for the following accredited units and learning elements

UNITS	ELEMENTS						
IFCA.U1	E1	E2	E3	E4	E5	E6	E7
IFCA.U2	E1	E2	E3				
IFCA.U3	E1	E2	E3	E4			
IFCA.U4	E1	E2	E3	E4			
IFCA.U5	E1	E2					

Date

Prof. (FH) Mag. Michael Reiner
President of ECQA

IA -Manager



LEGEND

IFCA.U1 Control Environment

- Integrity and Ethical Values (E1)
- Oversight Board (E2)
- Management's Philosophy and Operating Style (E3)
- Organizational Structure (E4)
- Financial Reporting Competencies (E5)
- Authority and Responsibility (E6)
- Human Resources (E7)

IFCA.U2 Risk Assessment

- Financial Reporting Objectives (E1)
- Financial Reporting Risks (E2)
- Fraud Risks (E3)

IFCA.U3 Control Activities

- Integration with Risk Assessment (E1)
- Selection and Development of Control Activity (E2)
- Policies and Procedures (E3)
- Information Technology (E4)

IFCA.U4 Information and Communication

- Financial Reporting Information (E1)
- Internal Control Information (E2)
- Internal Communication (E3)
- External Communication (E4)

IFCA.U5 Monitoring

- Ongoing and Separate Evaluations (E1)
- Reporting Deficiencies (E2)

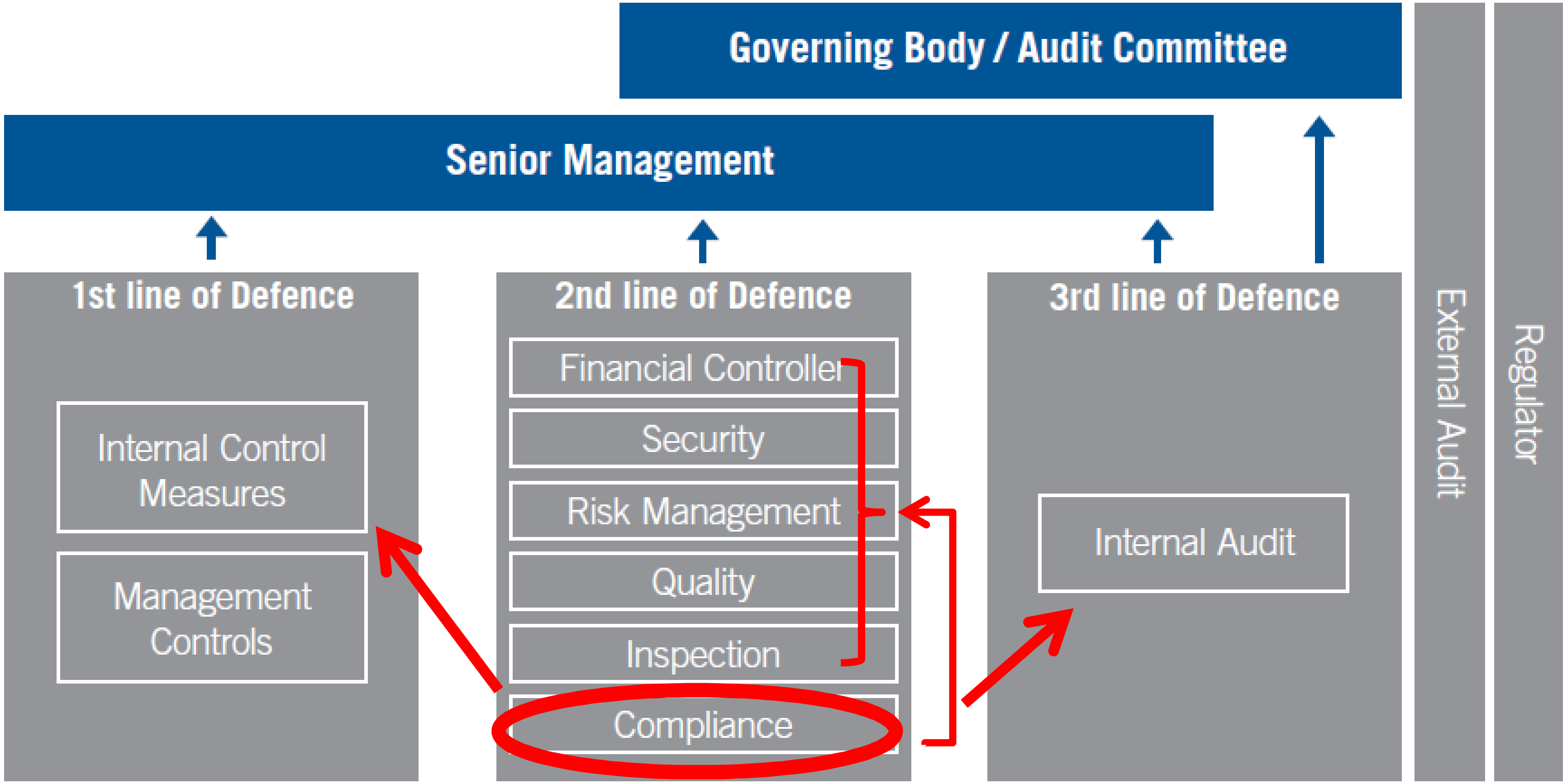
IA -Manager

issued by
European Certification and Qualification Association (ECQA)

Move forward (BPM-GOSPEL 2010-2013)

- From Compliance based Assurance to Enterprise Risk Management
- COBIT 5 – The Revised Control Framework Concept
- Trusted Business Model
  - Linking Governance Objectives to Enterprise Goals & Measures
  - Setting Governance Objectives
  - Enabling Processes
- Implementing Trusted Business Model
  - Case Studies for New Compliance Management Scenarios
  - ECQA certified Governance SPICE Assessor Skill Card
  - 2-level Qualification Scheme for Trusted Business
- Trusted Business and Effective Enterprise Governance
  - Validation of Governance SPICE Competencies for Trusted Business

The Compliance based ”Three Lines of Defence Model”

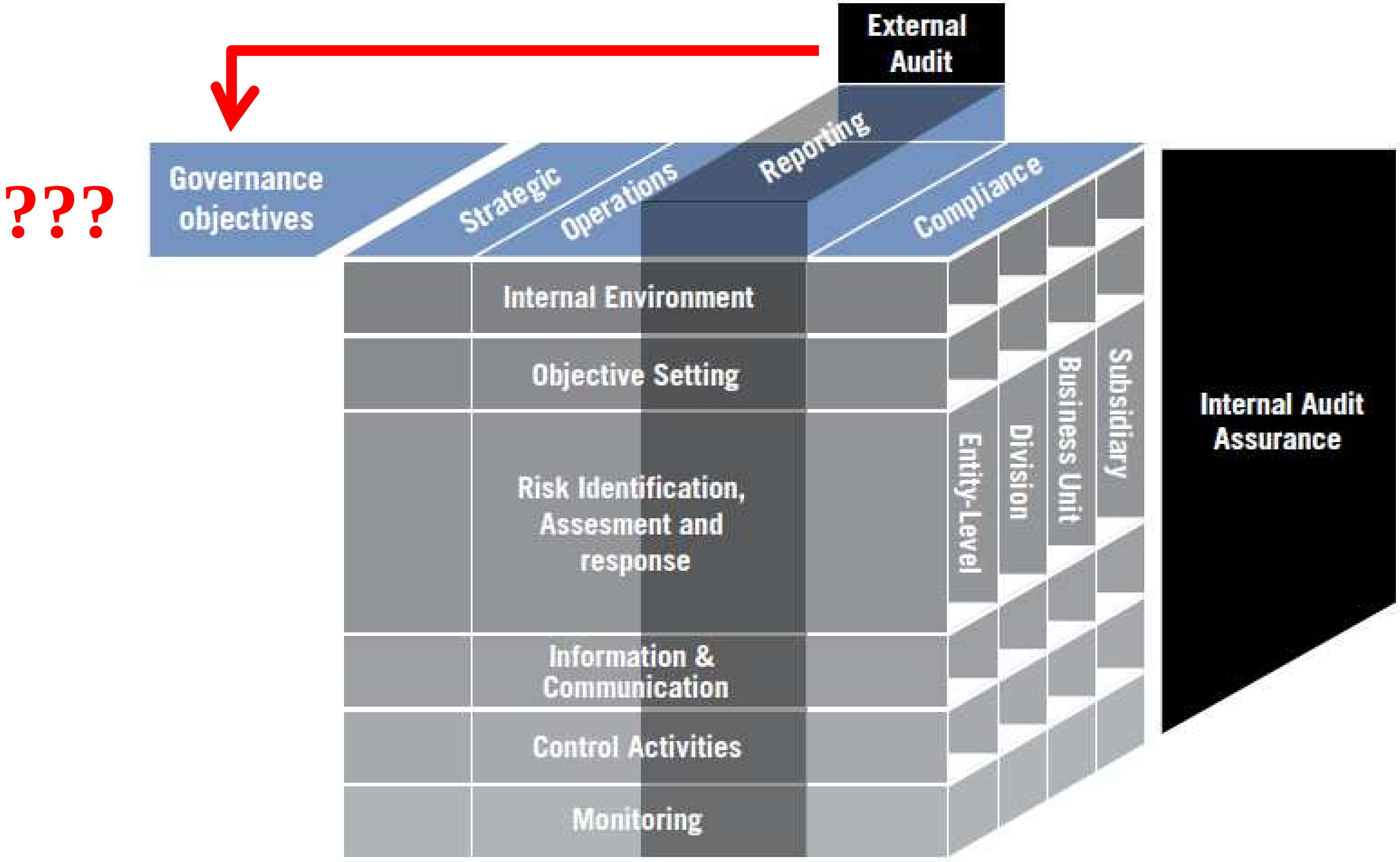


Source: ECIIA Corporate Governance Insights | May 2012

From Compliance based Assurance to Enterprise Risk Management

- No evidence that compliance drives business success (on the contrary: all big failure companies having had long list of compliance and excellence records)
- Managing compliance issues has only limited focus on lower level outcomes (e.g. activity goals)
- Enterprise Governance should focus on internal and external contexts of risks (ISO 31000: effects of uncertainties on enterprise objectives)
- Performance Measurement is needed for establishing useful risk criteria for supporting management decisions at all organizational and operational levels
- Measurement also helps managing compliance scenarios for validating risk treatment options

Enterprise Risk Management (COSO) and Control/Compliance based Assurance

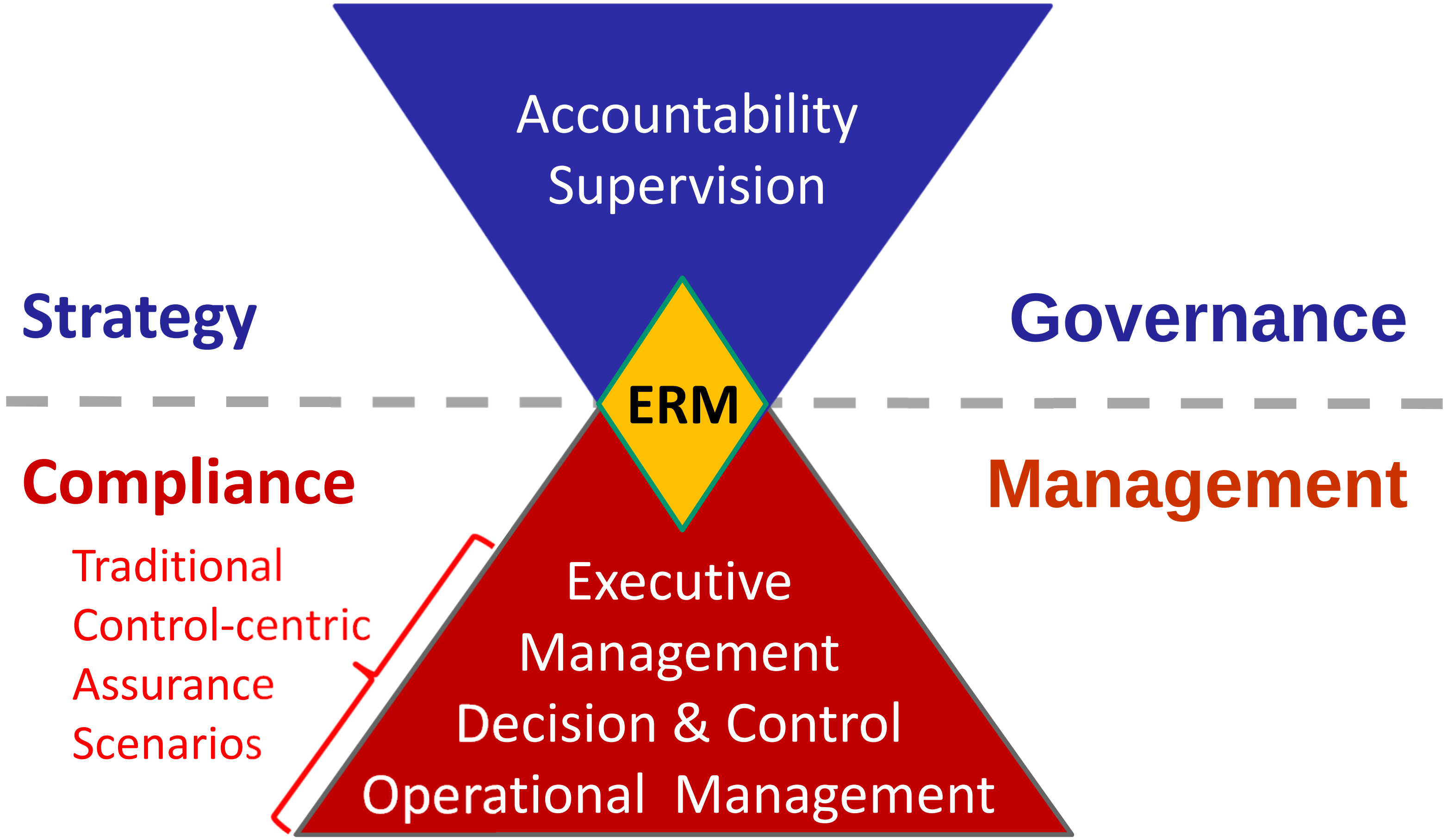


Source: ECIIA Corporate Governance Insights | May 2012

Why New Approaches are Needed?

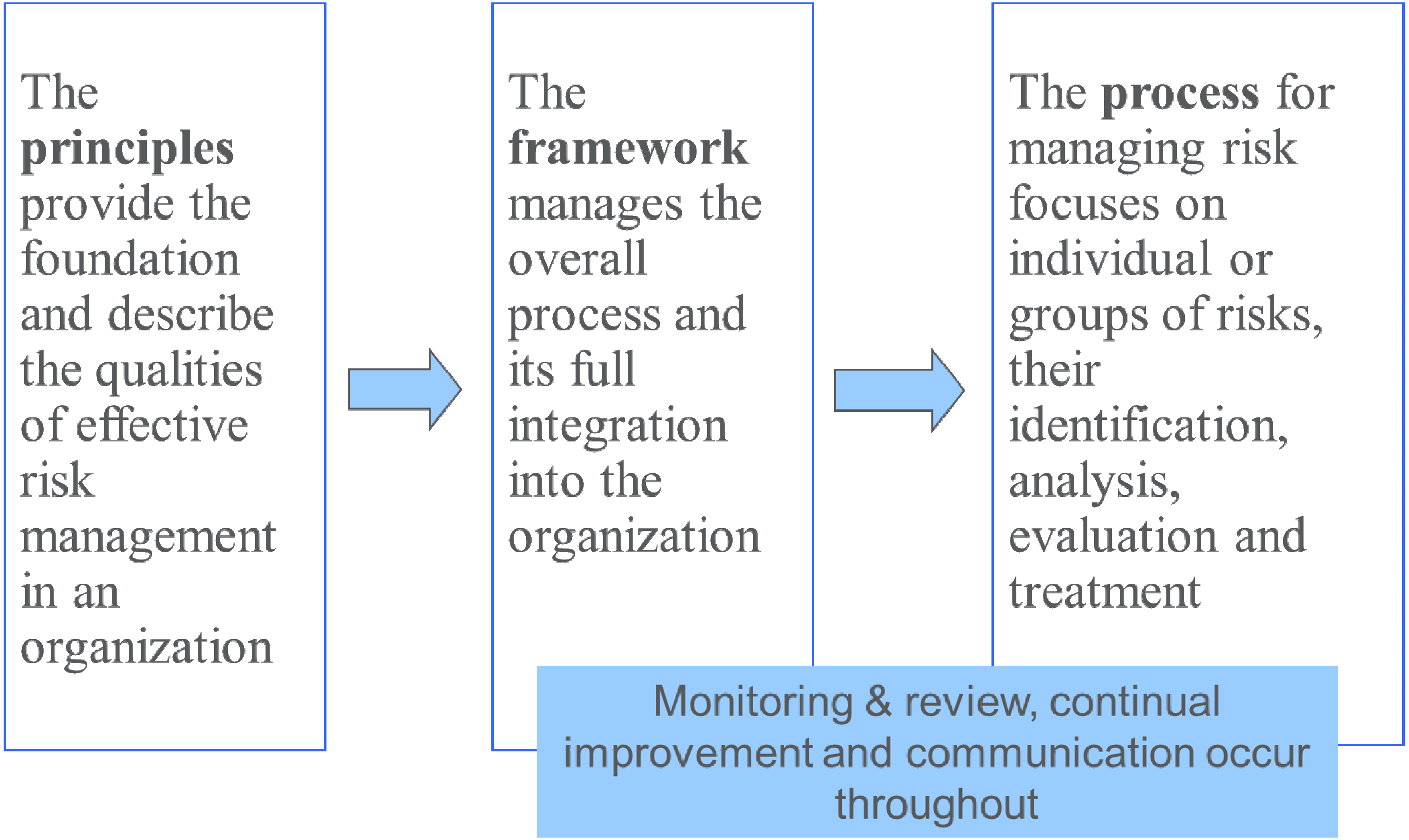
- The well established and recognized control frameworks and process reference models - like COSO and COBIT - could be used for effective and efficient enterprise governance, if only the management established its own governance related objectives.
- Unfortunately, structures of control frameworks and reference models are not easily interpretable by SME management for setting their business' specific governance objectives.
- Furthermore, the external and internal audit standards and literatures are also not really supportive in these terms.
- Adapting ISO 31000:2009 Risk Management Standard.

Risk Management's Role in Corporate Governance



By using figure of Kevin W. Knight: Incorporating AS/NZS ISO 31000:2009 Into Your ERM Strategies.

ISO 31000:2009 Risk Management



The **principles** provide the foundation and describe the qualities of effective risk management in an organization

The **framework** manages the overall process and its full integration into the organization

The **process** for managing risk focuses on individual or groups of risks, their identification, analysis, evaluation and treatment

Monitoring & review, continual improvement and communication occur throughout

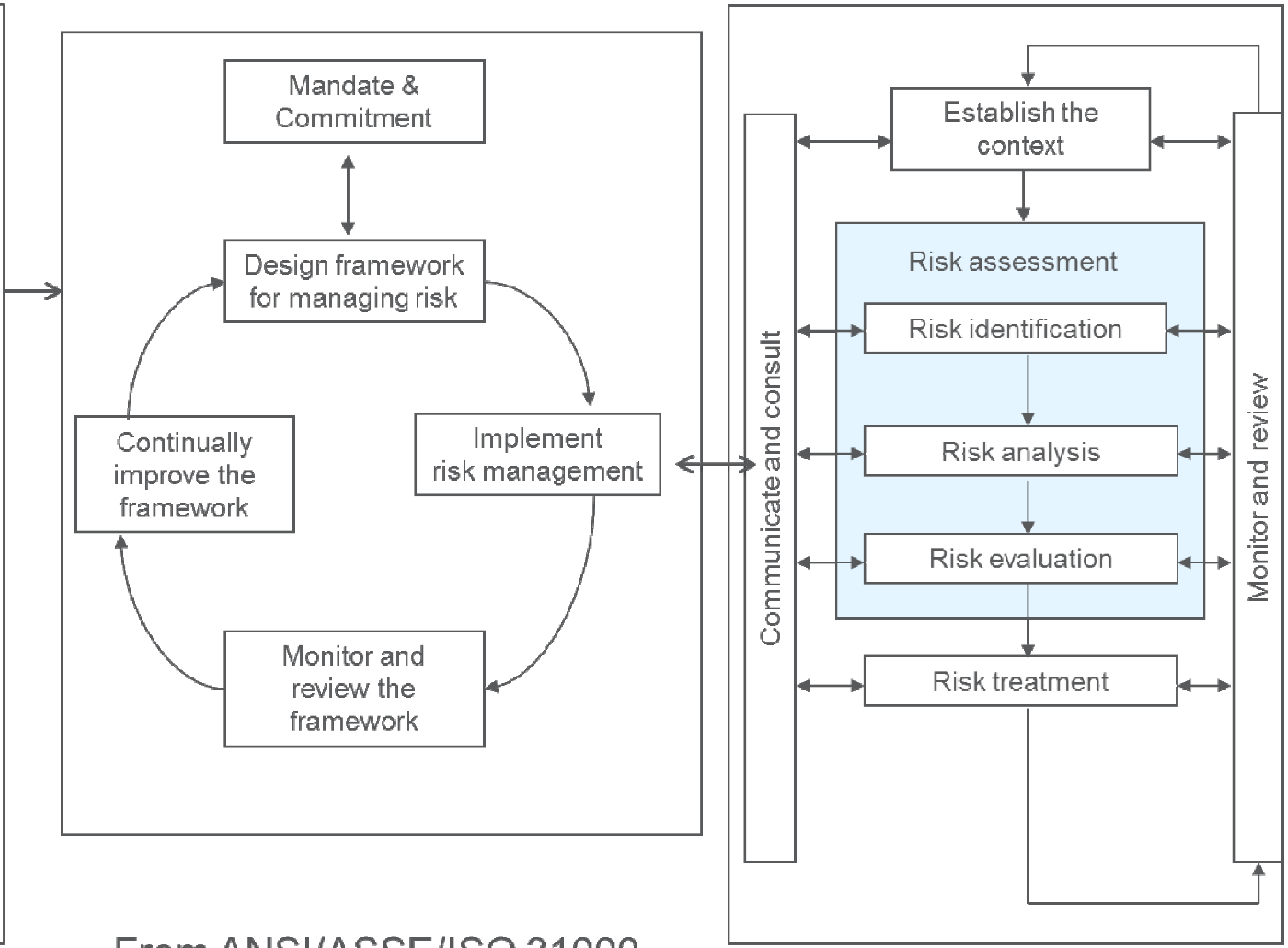
ISO 31000:2009 Risk Management

Principles

- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured & timely
- Based on best available info
- Tailored
- Takes human & cultural factors into account
- Transparent & inclusive
- Dynamic, iterative & responsive to change
- Facilitates continual improvement & enhancement of the org

Framework

RM Process

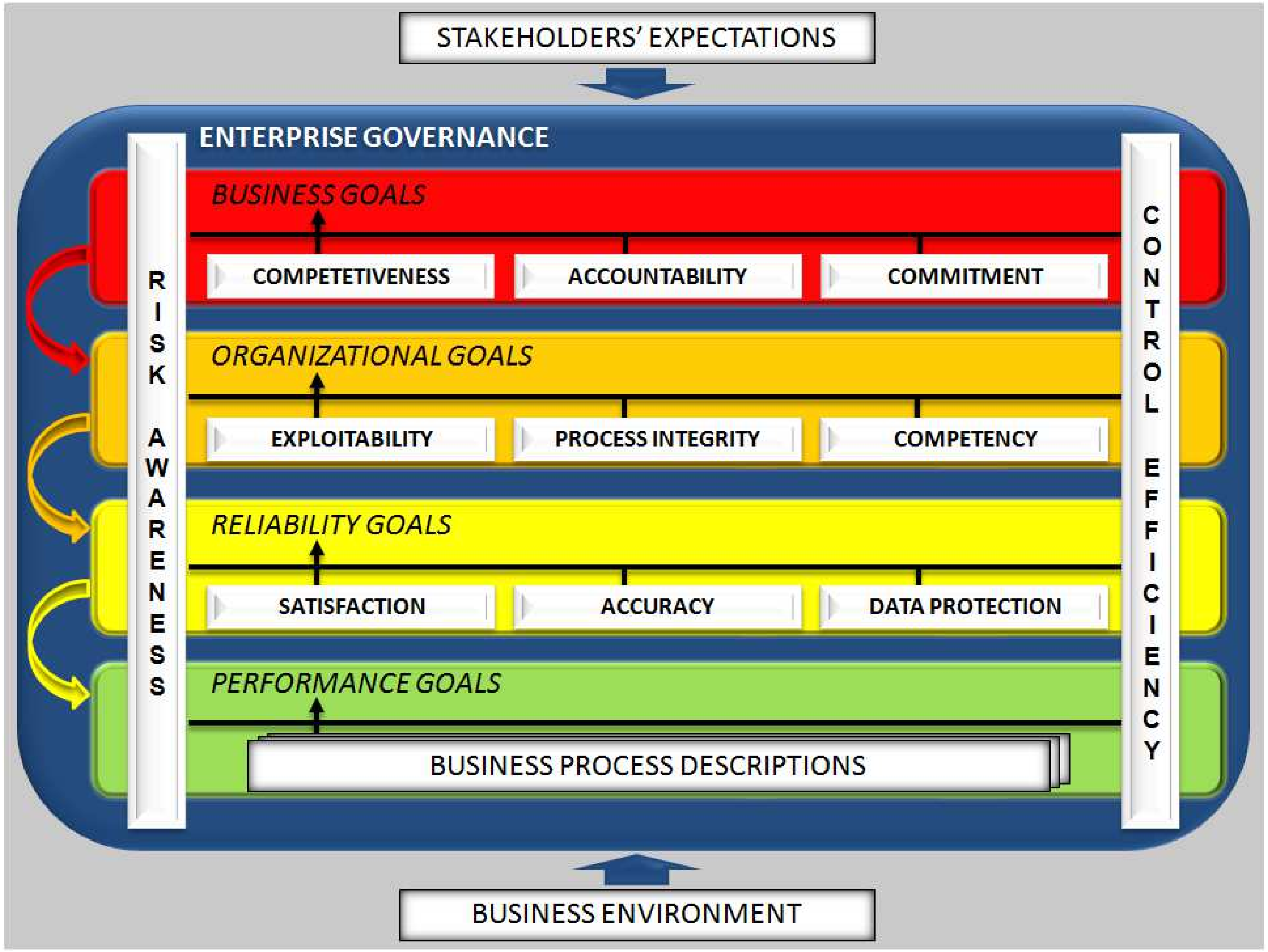


From ANSI/ASSE/ISO 31000

Trusted Business Model

- keeps both enterprise management and audit assurance logics in mind
- by presenting governance processes in line with the objectives relevant for enterprise management,
- together with an exact mapping to processes of control frameworks (reference models) accepted and used by auditors for compliance attestation.
- Provides description and application practices of governance processes for management assertions and assurance of trusted and sustainable business operation (internal context of risk management).
- Refers to best practices enabling achievement of governance objectives, instead of using them as compliance checklists.

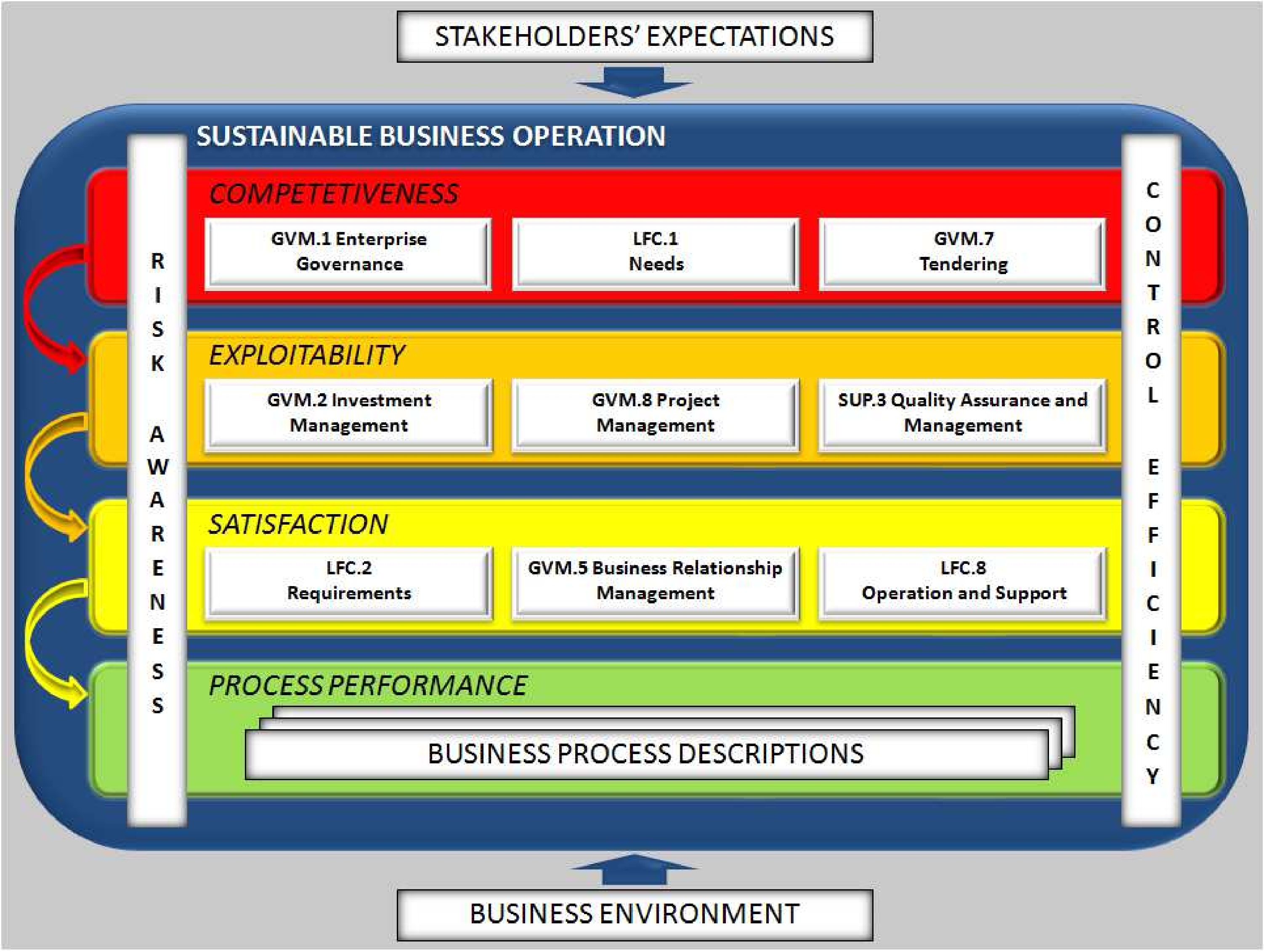
Linking Governance Objectives to Enterprise Goals & Measures



Trusted Business Model
Setting Governance Objectives

- Supporting Business Sustainability (leveraging opportunities)
  - Competitiveness (ESPICE)
  - Exploitability (ESPICE)
  - Satisfaction (ESPICE)
- Supporting Organization’s Internal Control System
  - Risk Awareness (COSO)
  - Accountability (COSO)
  - Competency (COSO)
  - Accuracy (COBIT, COSO)
  - Process Integrity (COSO)
  - Data Protection (COBIT, COSO, GAPP)
  - Commitment (COBIT, COSO)
  - Control Efficiency (COSO)

Enabling Processes and Practices for Sustainable Business Operation (ESPICE)



STAKEHOLDERS' EXPECTATIONS

SUSTAINABLE BUSINESS OPERATION

RISK AWARENESS

CONTROL EFFICIENCY

COMPETETIVENESS

- GVM.1 Enterprise Governance
- LFC.1 Needs
- GVM.7 Tendering

EXPLOITABILITY

- GVM.2 Investment Management
- GVM.8 Project Management
- SUP.3 Quality Assurance and Management

SATISFACTION

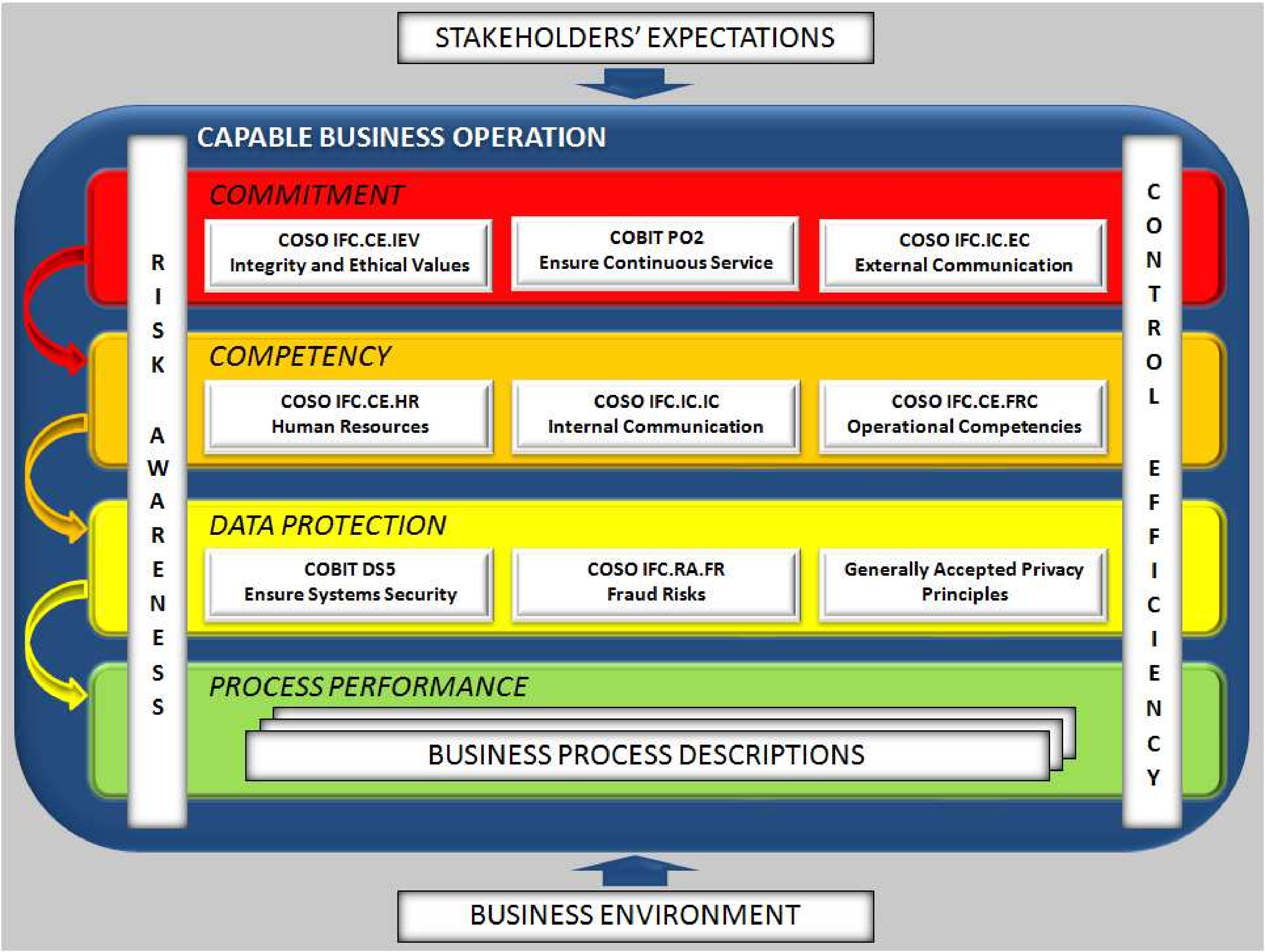
- LFC.2 Requirements
- GVM.5 Business Relationship Management
- LFC.8 Operation and Support

PROCESS PERFORMANCE

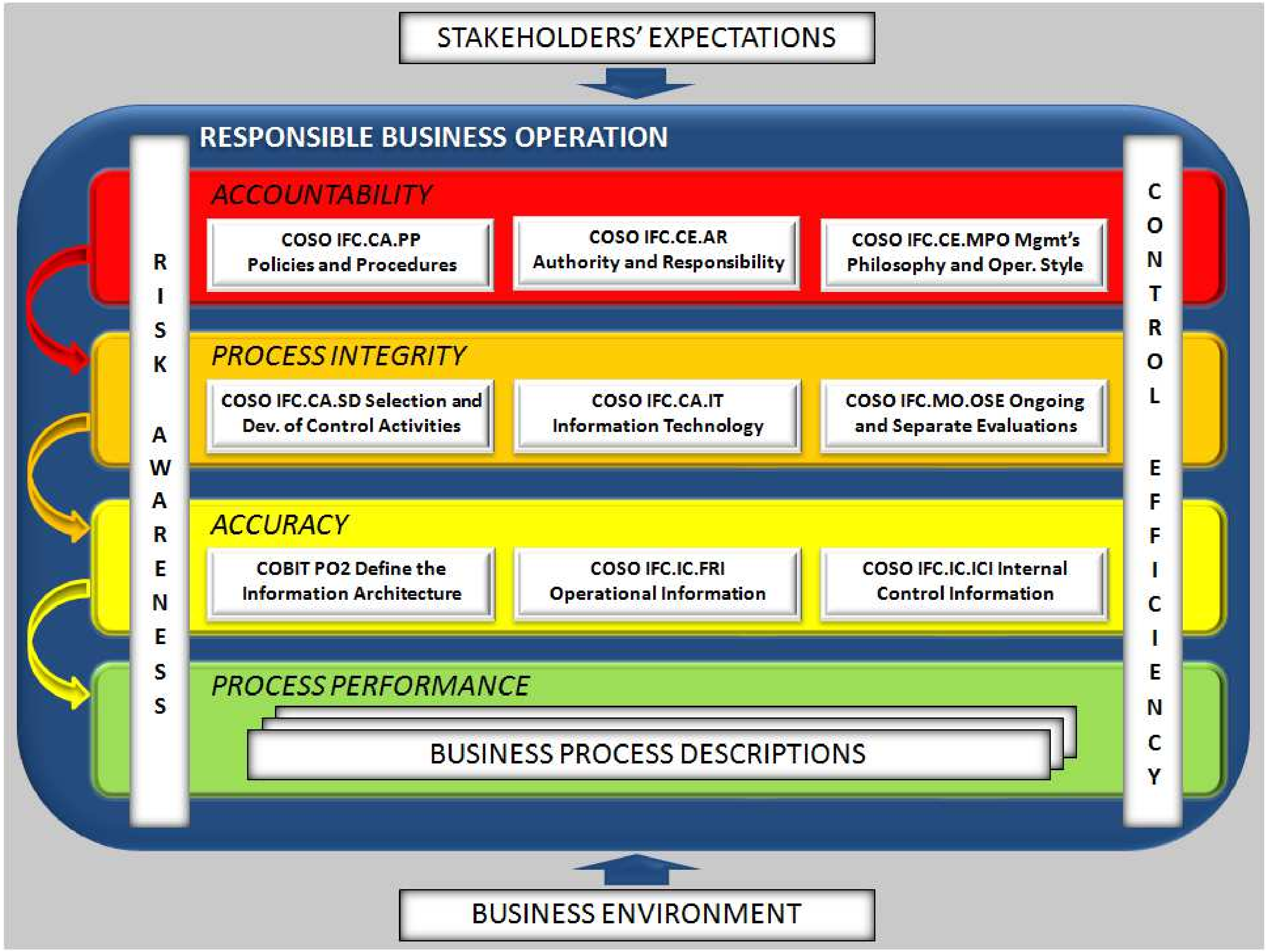
BUSINESS PROCESS DESCRIPTIONS

BUSINESS ENVIRONMENT

Enabling Processes and Practices for Capable Business Operation


STAKEHOLDERS' EXPECTATIONS
CAPABLE BUSINESS OPERATION
RISK AWARENESS
CONTROL EFFICIENCY
COMMITMENT
COSO IFC.CE.IEV Integrity and Ethical Values
COBIT PO2 Ensure Continuous Service
COSO IFC.IC.EC External Communication
COMPETENCY
COSO IFC.CE.HR Human Resources
COSO IFC.IC.IC Internal Communication
COSO IFC.CE.FRC Operational Competencies
DATA PROTECTION
COBIT DS5 Ensure Systems Security
COSO IFC.RA.FR Fraud Risks
Generally Accepted Privacy Principles
PROCESS PERFORMANCE
BUSINESS PROCESS DESCRIPTIONS
BUSINESS ENVIRONMENT

Enabling Processes and Practices for Responsible Business Operation



STAKEHOLDERS' EXPECTATIONS

RESPONSIBLE BUSINESS OPERATION

RISK AWARENESS

CONTROL EFFICIENCY

ACCOUNTABILITY

- COSO IFC.CA.PP Policies and Procedures
- COSO IFC.CE.AR Authority and Responsibility
- COSO IFC.CE.MPO Mgmt's Philosophy and Oper. Style

PROCESS INTEGRITY

- COSO IFC.CA.SD Selection and Dev. of Control Activities
- COSO IFC.CA.IT Information Technology
- COSO IFC.MO.OSE Ongoing and Separate Evaluations

ACCURACY

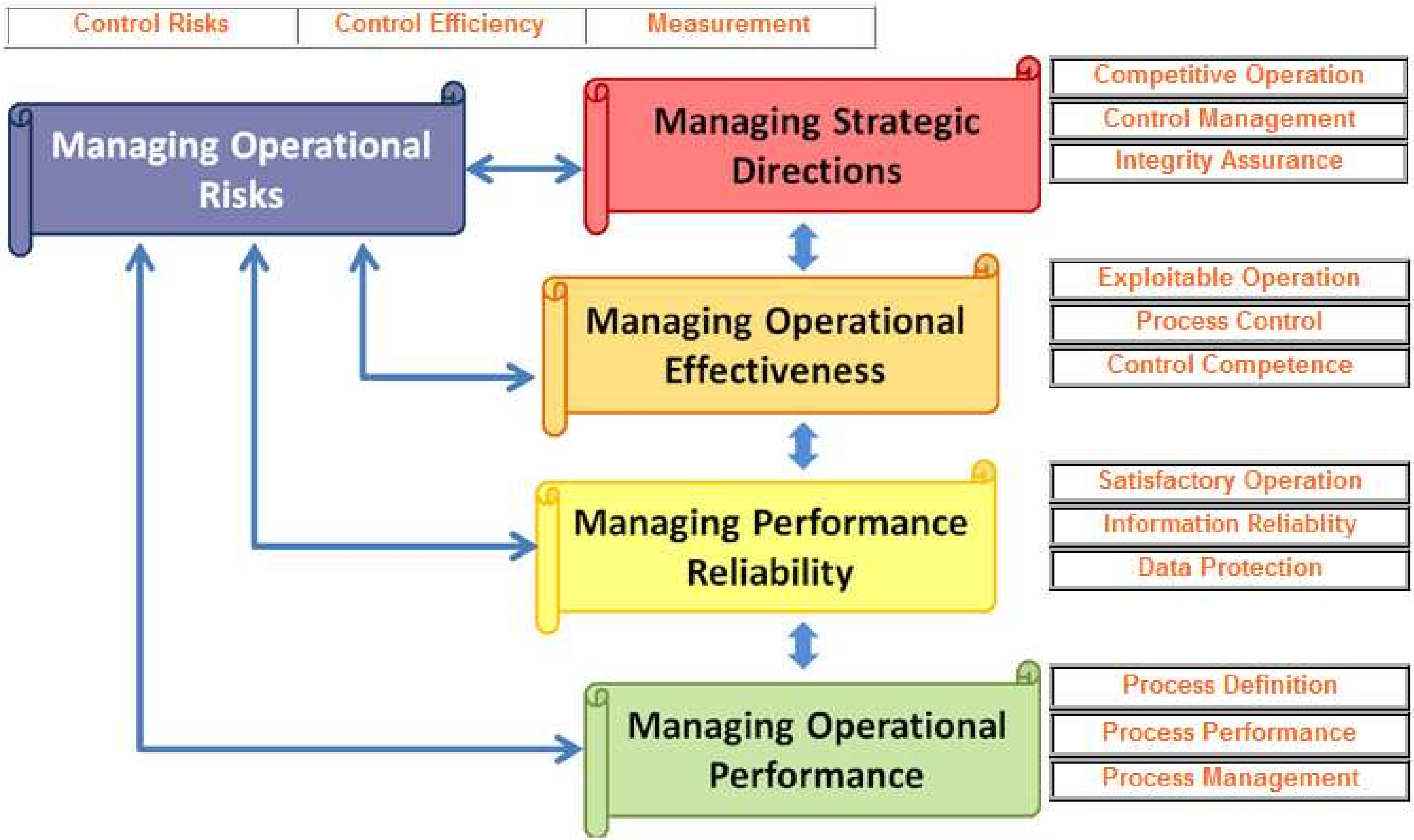
- COBIT PO2 Define the Information Architecture
- COSO IFC.IC.FRI Operational Information
- COSO IFC.IC.ICI Internal Control Information

PROCESS PERFORMANCE

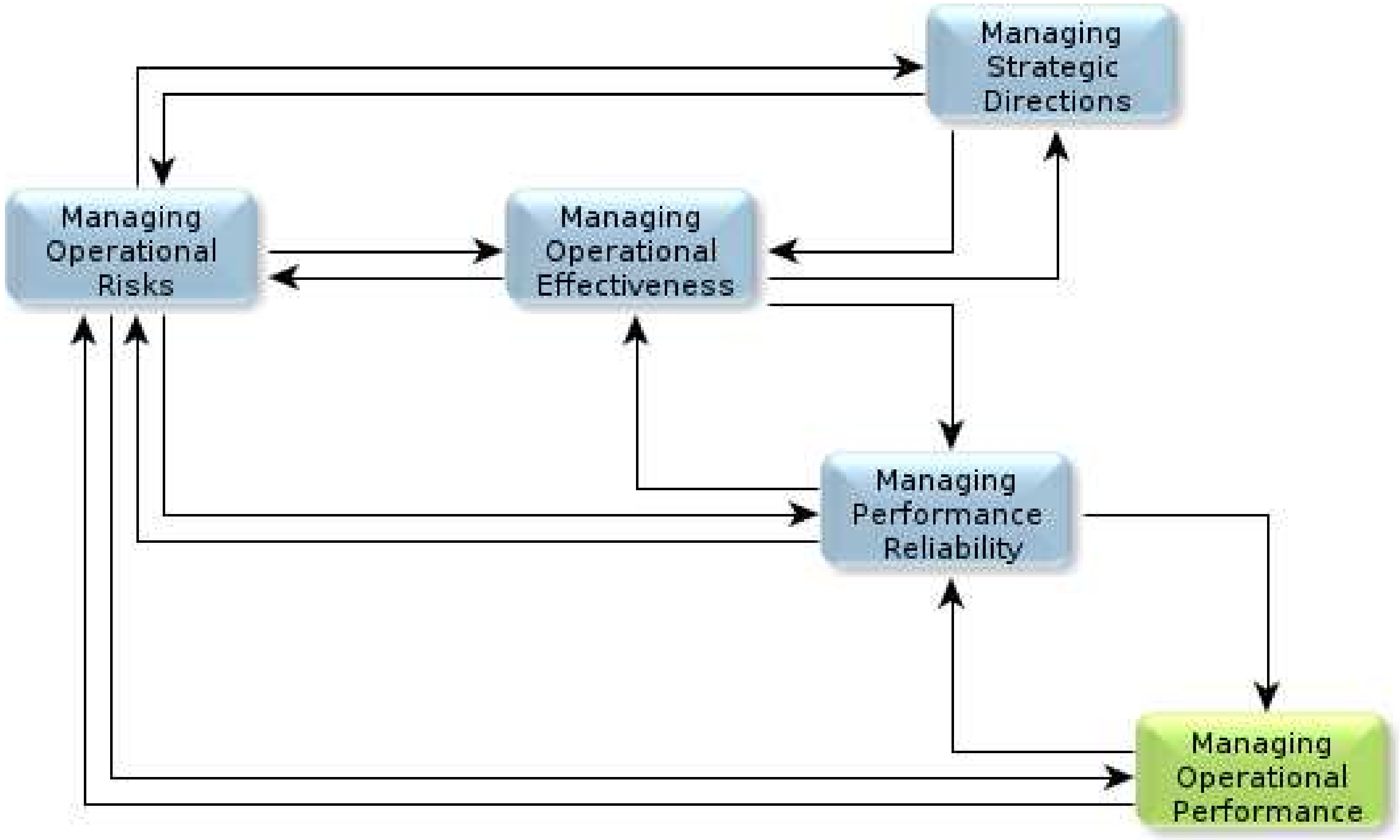
BUSINESS PROCESS DESCRIPTIONS

BUSINESS ENVIRONMENT

Integrated Assurance Management Scenarios



Governance Level 1: Performed Business Operation


Managing Strategic Directions
Managing Operational Risks
Managing Operational Effectiveness
Managing Performance Reliability
Managing Operational Performance

Managing Operational Performance 1.

Managing Operational Performance of those business processes that are relevant to perform the business operation in compliance with internal and/or external expectations, rules or regulations.

Roles:

- Responsible: Operational Manager
- Support: Risk & Compliance Manager, Staff
- Inform: Business Line Manager

Scope: Level 1- Performed Business Operation

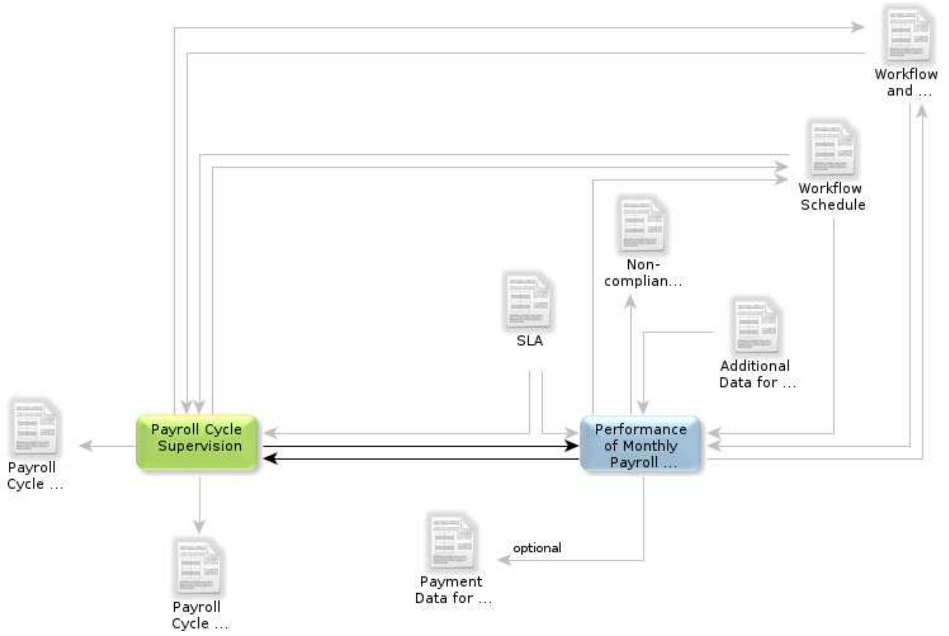
The organization demonstrates ability to manage performance of business processes that are relevant to support the organization’s business operation.

Managing Operational Performance 2.

Outcomes: The process capability dimensions of the performed business processes enable the organization:

- establishing operational plans for the performance of the relevant set of business processes supporting organization’s business operation;
- acting to ensure effective communication regarding the performance of the business processes, through clear assignment of responsibilities and authorities to involved parties;
- allocating adequate resources and information to ensure implementation of the operational plans;
- monitoring performance of the business processes against plans in the individual operational instances;
- taking action to address deviation from planned performance of the business processes;
- identifying compliance requirements for the management of outputs developed or maintained by the processes;
- taking action through appropriate reviews and control mechanisms to ensure that the compliance requirements for output management are satisfied.

Managing Operational Performance 3. Sample: Payroll Cycle Supervision



Roles

Responsible: Payroll Operation Manager
Support: IT contact, Payroll Controller, Payroll Clerk
Inform: Business Line Manager

Inputs

- Workflow Schedule
- Workflow and Document Tracking

Inputs from other Processes

- SLA

Outputs

- Workflow Schedule
- Workflow and Document Tracking

Outputs for other Processes

- Payroll Cycle Performance Report
- Payroll Cycle Control Summary Report

Description

Operational Management uses work-flow and documentation management system to supervise Monthly Payroll Calculation process activities and controls. Link to evidence

Managing Operational Performance 4. Sample metrics

Performance (”usefulness”)

Indicator: Performance Rate: *actual errorless calculations/planned calculations*

Time-horizon: operating cycles: *month of payroll processing*

Scale:

- approved major over performance: *over +10%*
- approved minor over performance: *+1-10%*
- approved performance at agreed levels: *+/- 1%*
- minor disapproval or indemnity: *1-5%*
- major disapproval or indemnity: *over 5%*

Expenditure (”effectiveness”)

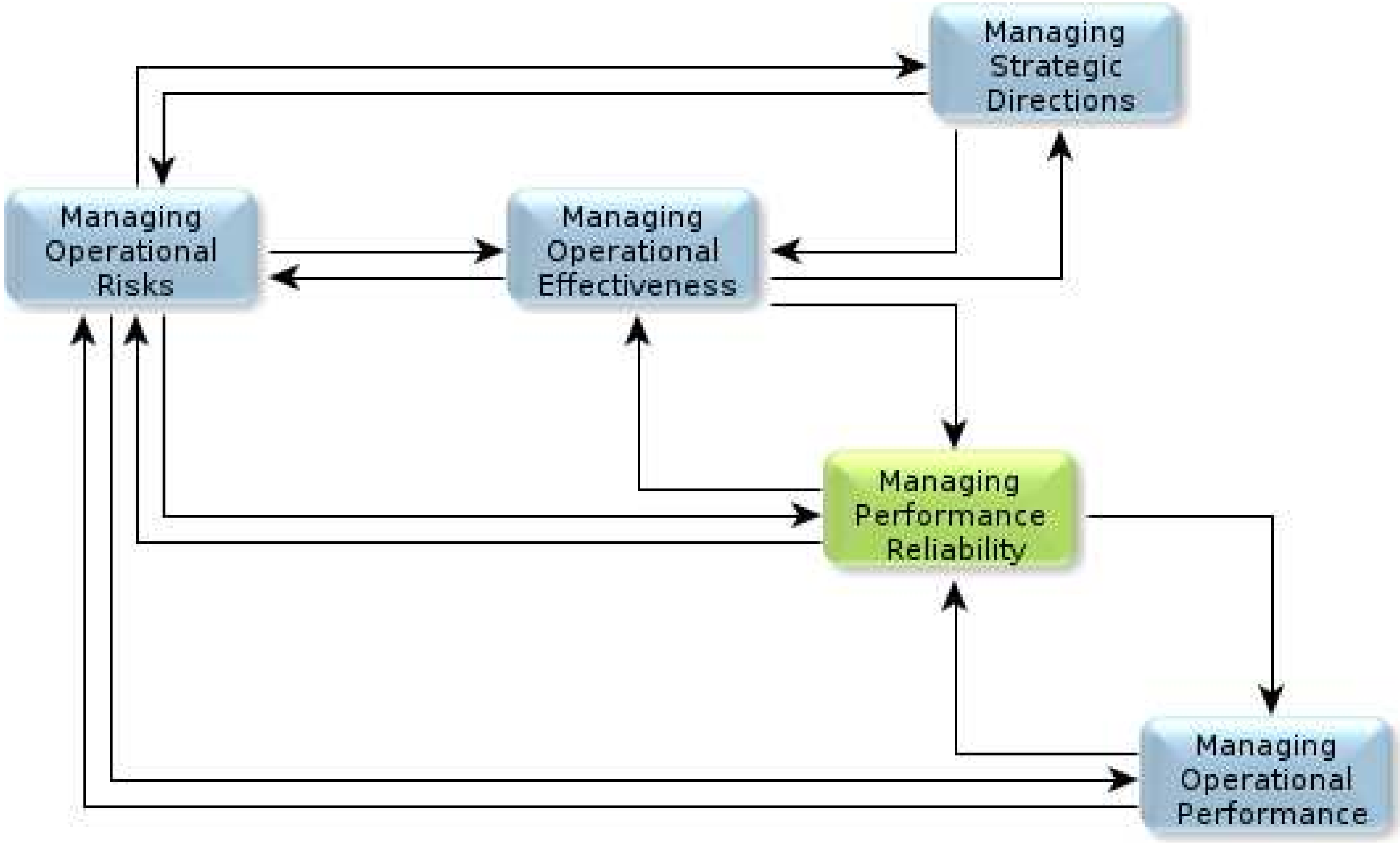
Indicator: Operating Costs: *hourly rate of payroll*

Time-horizon: operating cycles: *month of payroll processing*

Scale:

- significantly less than planned: *>15%*
- slightly less than planned: *5-15%*
- as planned: *+/- 5%*
- slightly more than planned: + *5-15%*
- significantly more than planned: over *+15%*

Governance Level 2: Reliable Business Operation


Managing Strategic Directions
Managing Operational Risks
Managing Operational Effectiveness
Managing Performance Reliability
Managing Operational Performance

Managing Performance Reliability 1.

Managing Performance Reliability to achieve satisfaction and trust of users/customers regarding operational performance.

Roles:

- Responsible: Business Line Manager
- Support: Risk & Compliance Manager, Operational Manager
- Inform: Business Unit Leader

Scope: Level 2 - Reliable Business Operation

The organization demonstrates ability to fulfill performance reliability requirements of business operation.

Managing Performance Reliability 2.

Outcomes: By the support of related governance practices, the organization:

- ensures user/customer satisfaction based on agreed levels of business operation;
- ensures the accuracy and consistency in data architecture and disclosure elements relevant for business operation, and for supporting data processing integrity;
- is committed to security, confidentiality and privacy principles to avoid unauthorized access to and misuse of confidential data effected by business operation.

Enablers:

- Adapting Satisfactory Operation practices
- Adapting Information Reliability practices
- Adapting Data Protection practices

Measures:

- Customer Retention (”usefulness”)
- Capacity Utilization (”effectiveness”)

Managing Performance Reliability 3. Sample metrics

Customer Retention (”usefulness”)

Indicator: Order Renewals

Time-horizon: contracting periods

Scale:

- extended orders
- intention to broaden (trust)
- affirmation (satisfaction)
- warnings (dissatisfaction)
- abandonment

Capacity Utilization (”effectiveness”)

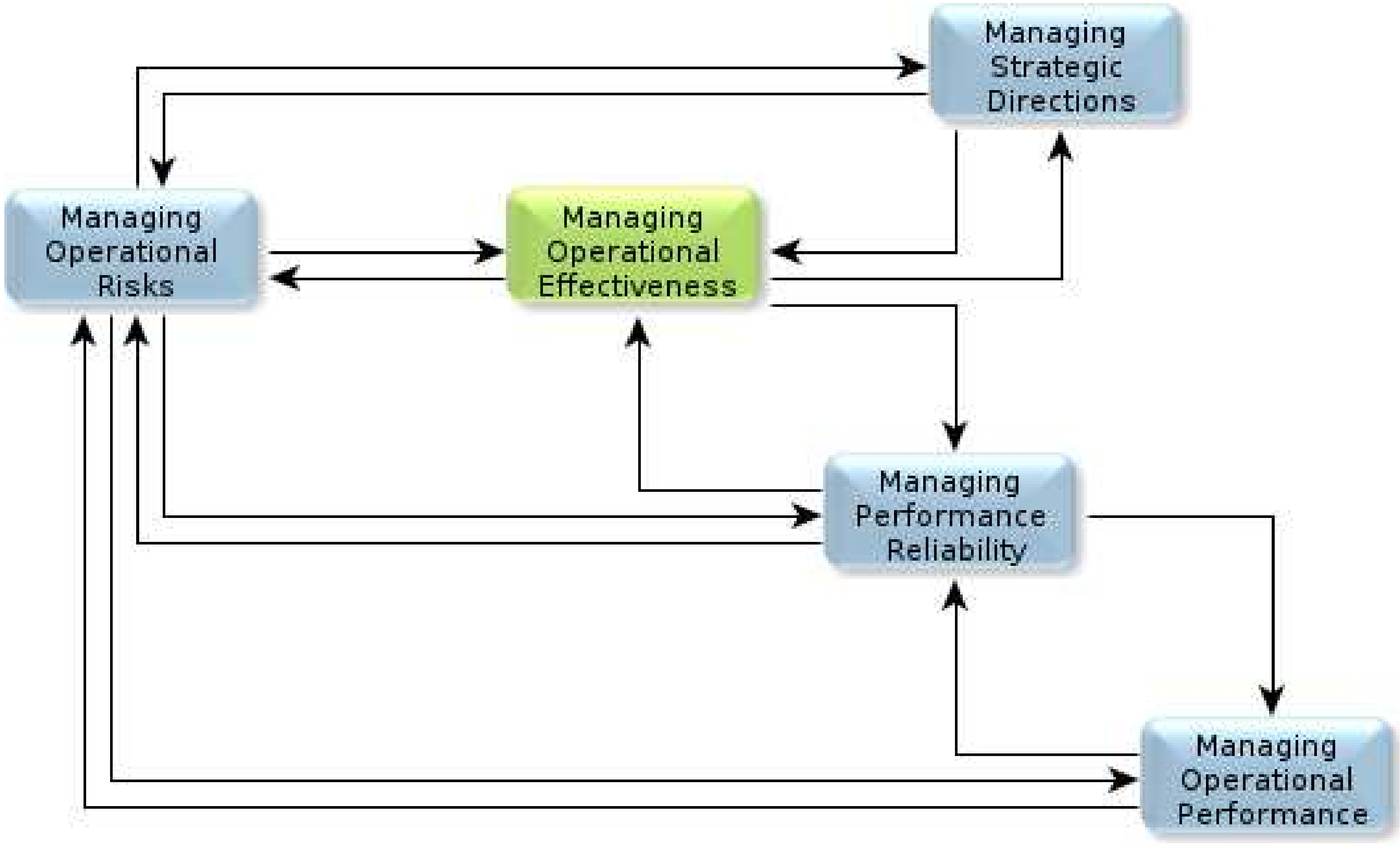
Indicator: Capacity Utilization Rate

Time-horizon: contracting periods

Scale:

- significantly better than planned
- better than planned
- as planned
- worse than planned
- significantly worse than planned

Governance Level 3:
Effective Business Operation


Managing Strategic Directions
Managing Operational Risks
Managing Operational Effectiveness
Managing Performance Reliability
Managing Operational Performance

Managing Operational Effectiveness 1.

Managing Operational Effectiveness to achieve specific operational performance objectives in alignment with organization's business goals.

Roles:

- Responsible: Business Unit Leader
- Support: Risk & Compliance Manager, Business Line Manager
- Inform: Executive Director

Scope: Level 3 - Effective Business Operation

The organization demonstrates ability to establish and achieve quantitative and qualitative performance objectives of business operation that are fundamental to support the organization’s relevant business goals.

Managing Operational Effectiveness 2.

Outcomes: By the support of related governance practices, the organization:

- realizes optimal value from business operation;
- effectively designs and operates process-level controls relevant to the objectives of business operation, and processing integrity principle;
- makes sufficient skills and knowledge relevant for the objectives of business operation available and effectively used.

Enablers:

- Adapting Exploitable Operation practices
- Adapting Process Control practices
- Adapting Competence Control practices

Measures:

- Profitability (”usefulness”)
- Agile Resource Allocation (”effectiveness”)

Managing Operational Effectiveness 3. Sample metrics

Profitability (”usefulness”)

Indicator: Operating Margin

Time-horizon: reporting periods

Scale:

- significantly over achieved
- moderately over achieved
- achieved as planned
- moderately underachieved
- significantly underachieved

Agile Resource Allocation (”effectiveness”)

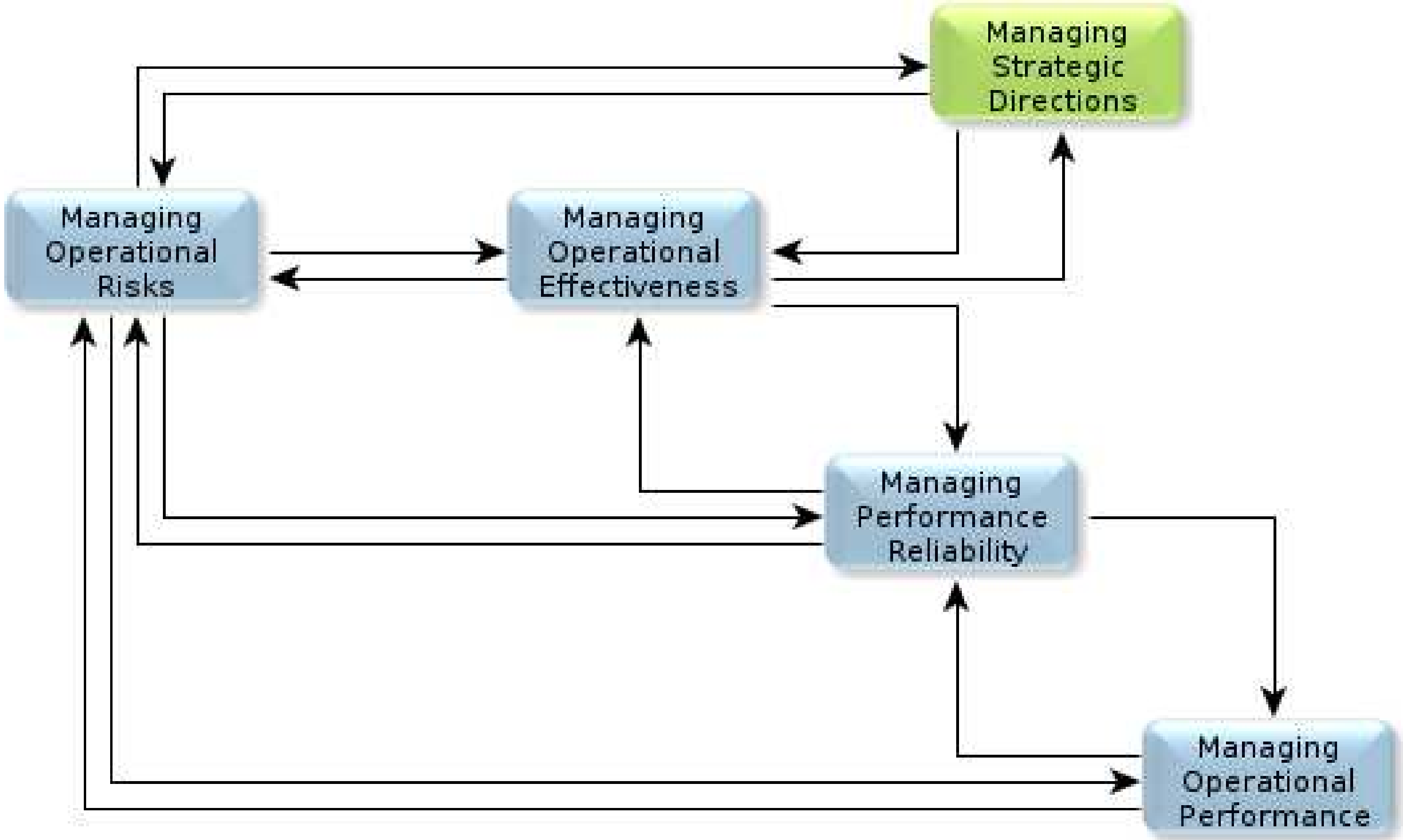
Indicator: Unit Cost

Time-horizon: reporting periods

Scale:

- very low variance
- variance within acceptable limits
- affordable variance
- more than affordable variance
- too high variance

Governance Level 4: Strategic Business Operation


Managing Strategic Directions
Managing Operational Risks
Managing Operational Effectiveness
Managing Performance Reliability
Managing Operational Performance

Managing Strategic Directions 1.

Managing Strategic Directions in order to establish and maintain corporate commitment aligned with stakeholder's needs and expectations.

Roles:

- Responsible: Executive Director
- Support: Risk & Compliance Manager, Business Unit Leader
- Inform: Board, External Stakeholders

Scope: Level 4 - Strategic Business Operation

The organization demonstrates the ability to establish commitment for consistent and predictable performance of successful business operation aligned with strategic corporate objectives.

Managing Strategic Directions 2.

Outcomes: By the support of related governance practices, the organization:

- ensures market recognition of the business operation;
- makes management accountable for business operation in a way which is aligned with strategic corporate objectives;
- is committed to comply with ethical and integrity, business continuity and transparency requirements relevant to the stakeholders' needs and expectations.

Enablers:

- Adapting Competitive Operation practices
- Adapting Control Management practices
- Adapting Integrity Assurance practices

Measures:

- Business Goals (”usefulness”)
- Funding Resources (”effectiveness”)

Managing Strategic Directions 3.
Sample metrics

Business Goals (”usefulness”)

Indicator: Revenues

Time-horizon: strategic planning periods

Scale:

- significantly over achieved
- moderately over achieved
- Achieved
- moderately underachieved
- significantly underachieved

Funding Resources (”effectiveness”)

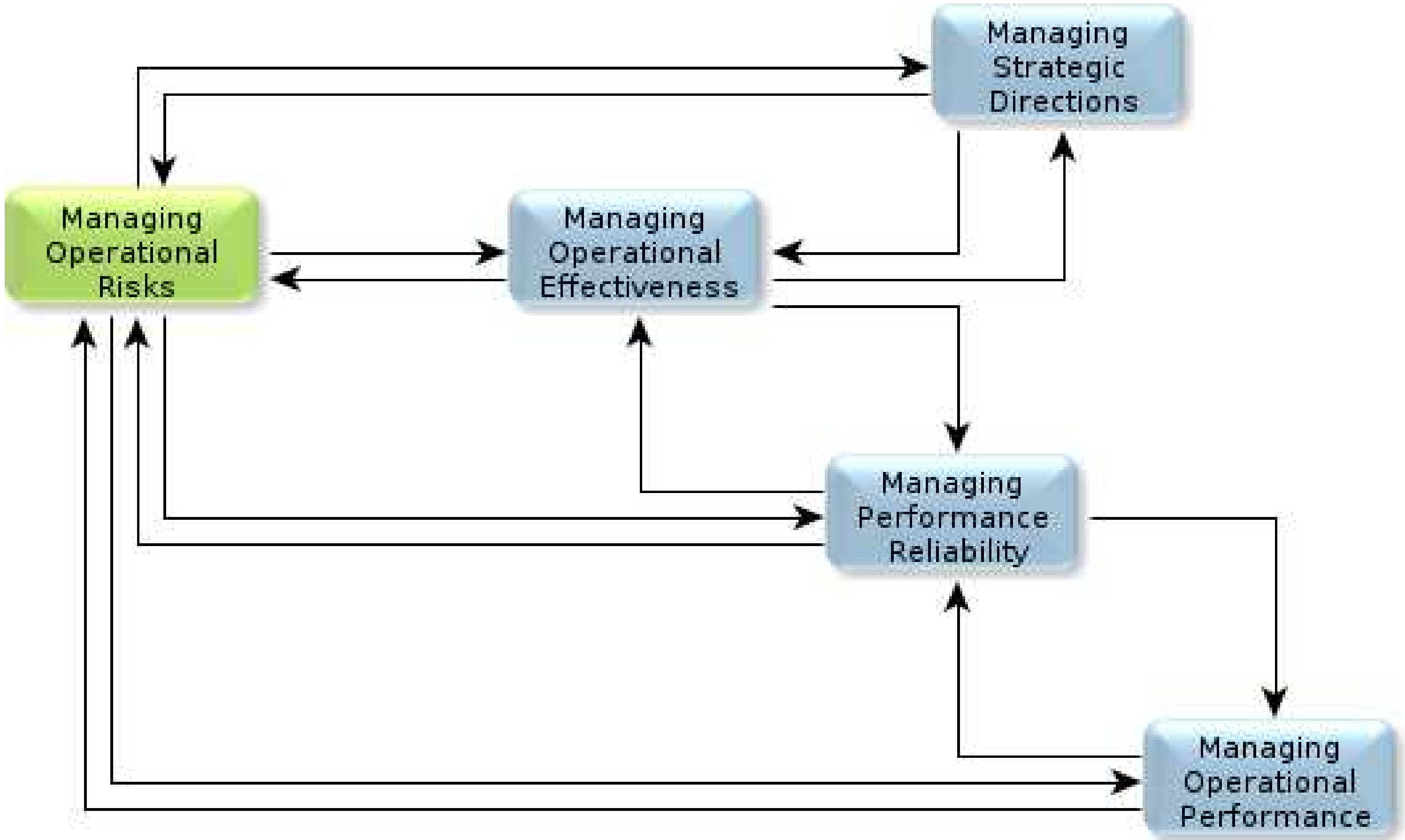
Indicator: Cash Flow

Time-horizon: strategic planning periods

Scale:

- available financial resources for approved requests over plan
- limited financial resources for non-planned requests
- financial resources are available for planned requests in a predictable manner
- availability of financial resources is less predictable or lagged behind the plan
- permanent and/or significant lack of financial resources

Enterprise Governance over Business Operation: Managing Operational Risks


Managing Strategic Directions
Managing Operational Risks
Managing Operational Effectiveness
Managing Performance Reliability
Managing Operational Performance

Managing Operational Risks 1.

Managing Operational Risks to facilitate business operation in achievement of business goals.

Roles:

- Responsible: Risk & Compliance Manager
- Support: Trusted Business Advisor
- Inform: Board, Executive Director

Scope: Level 1-4 of Enterprise Governance

The organization demonstrates the ability to manage risks related to business operation that are fundamental to select and implement governance practices as risk treatment options leveraging achievement of organization’s business goals established for business operation.

Managing Operational Risks 2.

Outcomes: By the support of related governance practices, the organization:

- takes communication and consultation with external and internal stakeholders during all stages of the risk management;
- establishes the internal and external context of business operation and risk management;
- identifies, analyzes and evaluates risks related to business operation;
- performs risk treatment cycles of providing or modifying controls and assessing their effectiveness against tolerable risk levels;
- takes periodic or ad hoc monitoring and review activities.

Enablers:

- Adapting Control Risks practices
- Adapting Control Efficiency practices

Measures:

- Effective Governance (”usefulness”)
- Consulting and Assurance Expenditure (”effectiveness”)

Managing Operational Risks 3. Sample metrics

Effective Governance (”usefulness”)

Indicator: Governance Capability Levels (actual vs. target)

Time-horizon: reporting periods

Scale:

- significantly over achieved
- moderately over achieved
- achieved as targeted
- moderately underachieved
- significantly underachieved

Consulting and Assurance Expenditure (”effectiveness”)

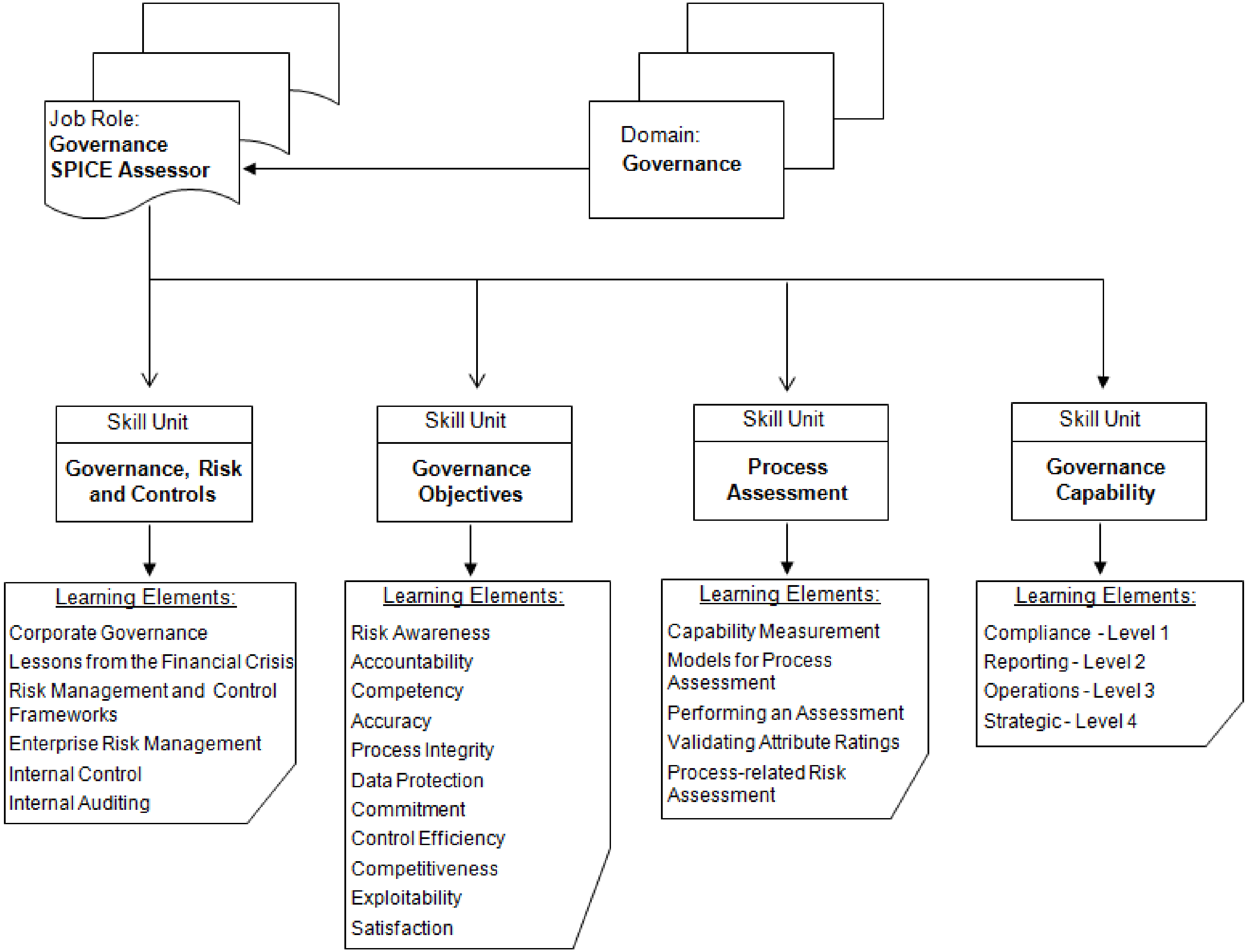
Indicator: Consulting and Assurance Costs

Time-horizon: reporting periods

Scale:

- significantly less than planned
- slightly less than planned
- as planned
- slightly more than planned
- significantly more than planned

Implementing the Governance SPICE Assessor Certification Scheme



Job Role: **Governance SPICE Assessor**

Domain: **Governance**

Skill Unit: **Governance, Risk and Controls**

Learning Elements:
- Corporate Governance
- Lessons from the Financial Crisis
- Risk Management and Control Frameworks
- Enterprise Risk Management
- Internal Control
- Internal Auditing

Skill Unit: **Governance Objectives**

Learning Elements:
- Risk Awareness
- Accountability
- Competency
- Accuracy
- Process Integrity
- Data Protection
- Commitment
- Control Efficiency
- Competitiveness
- Exploitability
- Satisfaction

Skill Unit: **Process Assessment**

Learning Elements:
- Capability Measurement
- Models for Process Assessment
- Performing an Assessment
- Validating Attribute Ratings
- Process-related Risk Assessment

Skill Unit: **Governance Capability**

Learning Elements:
- Compliance - Level 1
- Reporting - Level 2
- Operations - Level 3
- Strategic - Level 4

How SMEs (should) implement Effective Governance?

Less isolated risk & compliance management programs

- More responsibility of the ”Executive” level management
- Set links between strategic business objectives and management control processes
- Integrated assessment/audit approaches

Transparency

- Applying business objectives for managing/supervising compliance programs
- Presenting excellence in an understandable way (format)
- Using competent and qualified human resources
- Assuring accuracy by harmonizing time horizons to business objectives

Coverage

- Defining the business operation boundary conditions
- Leveraging the business opportunities (sustainability)
- Addressing the sector-specific technical/regulatory (control) requirements of the core business activities

Information and Contact

- www.governancecapability.com (English)
- www.training.ia-manager.org (English&Hungarian)
- www.trusted.hu (Hungarian)

Contact: János Ivanyos, ivanyos@trusted.hu

Thank you for your attention!