Governance SPICE Model

used by the

Internal Financial Control Assessor

Training Programme

Contact:
János Ivanyos
Memolux Ltd.
+36 1 467403
ivanyos@memolux.hu
www.training.ia-manager.org

www.ecqa.org
Topics

• “Governance” SPICE
• COSO Frameworks
• Setting Objectives in Enterprise Risk Management
• COBIT Performance Measurement
• COSO Objective Categories
• COSO-SPICE Performance Measurement
• Mapping COSO Objectives with Capability Levels
• COSO & COBIT as Process Reference Models
• Control Risk Assessment
• Supporting Effectiveness Conclusion on Internal Controls
• Key Controls: Applying Organizational Maturity concept
“Governance” SPICE

Refers to

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

- Terminology database
- Ontology model
Validation of Governance SPICE Competencies

Assessors

demonstrate their

Assessments

to carry out!

Competence

results from

Knowledge of the process and application domain

is gained by

Education

Skills in the principle technologies of ISO/IEC 15504

are gained by

Training

Personal attributes that contribute to effective performance

is gained by

Experience

indicates

Validation

Governance, Risk and Controls

Audit

SPICE
Application Domain

GENETIC ENGINEERING?

NO, CREATIVE ACCOUNTING
Corporate Governance Breakdowns

- The board of directors **failed to understand the risks** that the firm was taking, and did not exercise appropriate oversight or questioning of senior managers’ and employees’ actions;
- **Conflicts of interest** and a lack of independent board members and senior executives resulted in decisions that benefited a few at the expense of the many;
- **Internal controls** were either weak or non-existent, or appeared to be adequate on paper but were not implemented in practice;
- **Internal and external audit** “fell asleep at the switch” and failed to detect fraudulent behaviour, and in some cases even aided and abetted such behaviour;
- **Transactions and organisational structures** were designed to reduce transparency and prevent market participants and regulators from gaining a genuine picture of the firm’s condition;
- The **corporate culture** fostered unethical behaviour and discouraged questions from being raised.

by Mr Jaime Caruana, Governor of the Bank of Spain and Chairman of the Basel Committee on Banking Supervision, at the 2nd Islamic Financial Services Board (IFSB) Summit 2005
A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.
Welcome

COSO is recognized the world over for providing guidance on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting. We hope you find the information on this site to be helpful and we welcome your input on any COSO drafts exposed for comment.

What's New

**Guidance on Monitoring Internal Control Systems**

COSO is pleased to release the first volume of its monitoring guidance — the *Introduction*. This business guidance more fully develops the monitoring component of the *Internal Control - Integrated Framework* to assist companies in ensuring the effectiveness of their financial, operational, and compliance-related internal controls.

More>>
Common Principles based on Internal Controls

• Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework, 1992
• INTOSAI: Guidelines for Internal Control Standards for the Public Sector, 2004
• Basle Committee on Banking Supervision: Framework for Internal Control Systems in Banking Organisations, 1998
• COSO: Enterprise Risk Management — Integrated Framework, 2004
• SOX, Company Law in the EU, Corporate Governance Codes, etc.

Following the supervisory, external and internal audit principles on internal control systems, the Internal Financial Control Assessment model refers to the principles of the COSO 2006 Guidance
COSO IC and ERM Frameworks supporting management and control systems

Source: www.coso.org
Components of Internal (Financial) Control System

1. **Set (Financial Reporting) Objectives**
   - Once Effective Control is established, develop Monitoring activities to ensure that controls continue to operate effectively.
   - Develop Effective Information & Communication to Assist Organization in Meeting its Objectives
   - Design & Implement Effective Control Activities to address risks

2. **Identify Risks to the Achievement of those Objectives**
   - Design & Implement an Effective Control Environment as First Line of Defense against the Risks

3. **Effective Internal Control (Over Financial Reporting)**
   - Key risks analysis

Determine effectiveness
“… a **process**, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its **risk appetite**, to provide **reasonable assurance** regarding the achievement of **entity objectives**.”

In COSO Enterprise Risk Management (ERM) terminology, the management considers risks strategy in the setting of objectives, such as:

– **Risk Appetite** of the entity - a high-level view of how much risk the management and the board are willing to accept.

– **Risk Tolerance** - the acceptable level of variation around objectives - is aligned with risk appetite.
Objectives setting (cont.)

- Entity or operational unit level **objectives with their acceptable variations** should be defined by using adequate metrics (indicators). Normally this is not difficult as business objectives of any organization or operational processes represent - easily quantifiable - value creation or protection.

- However the **quantification of risk appetite** (crucial for risk management) is not evidential. The importance of the problem is derived from that risk appetite is the base for ranking risks during risk assessment for supporting the decision on **selecting of the potential risk responses**.
Identify Risk Responses

- Quantification of risk exposure

- Options available:
  - Accept = monitor
  - Avoid = eliminate \((\text{get out of situation})\)
  - Reduce = institute controls
  - Share = partner with someone \((\text{e.g. insurance})\)

- Residual risk \((\text{unmitigated risk – e.g. shrinkage})\)
Impact vs. Probability

<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High Risk</td>
<td>Mitigate &amp; Control</td>
</tr>
<tr>
<td>High</td>
<td>Medium Risk</td>
<td>Share</td>
</tr>
<tr>
<td>High</td>
<td>Low Risk</td>
<td>Accept</td>
</tr>
<tr>
<td>Low</td>
<td>Medium Risk</td>
<td>Control</td>
</tr>
</tbody>
</table>

**High Risk**

**Medium Risk**

**Low Risk**

**Accept**

**Share**

**Control**
## Example: Call Center Risk Assessment

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>PROBABILITY</th>
<th>Low Risk</th>
<th>Medium Risk</th>
<th>High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>• Fraud</td>
<td>• Entry errors</td>
<td>• Credit risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lost transactions</td>
<td>• Equipment obsolescence</td>
<td>• Customer has a long wait</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Employee morale</td>
<td>• Repeat calls for same problem</td>
<td>• Customer can’t get through</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Customer can’t get answers</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>• Loss of phones</td>
<td>• Entry errors</td>
<td>• Credit risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Loss of computers</td>
<td>• Equipment obsolescence</td>
<td>• Customer has a long wait</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Repeat calls for same problem</td>
<td>• Customer can’t get through</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Customer can’t get answers</td>
<td>• Customer can’t get answers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Setting Target for Internal Control Objectives (Cost vs. Benefit)
Setting Risk Appetite for Internal Controls

EFFECTIVENESS OF PROTECTION

$\text{RISK}$

$\text{COST}$

Risk Tolerance

Tolerable Risk Point

Possible Risk Appetite
Increasing Efficiency of Internal Controls

EFFECTIVENESS OF PROTECTION

TARGET = Tolerable Risk Point
by automation or radical changes

Risk Tolerance

EFFECTIVENESS OF PROTECTION

RISK

COST

COST

www.ecqa.org © ecqa 2009
The COSO ERM model – integrating the internal control system – sets objective categories. The strategic, operations, reporting and compliance objectives should be investigated through the achievement of business objectives concerning either the organization (in ERM), or the operational units and processes (in case of integrated internal control system).

Though different (performance, financial, or compliance) audit types can be defined based on the objective categories, it is evidential that these categories can exist only in interconnection.
Measuring Objectives

- The consistent enterprise risk management presumes that the operation of internal control system of the organization is measurable by adequate indicators.
- These indicators play roles in setting objectives regarding internal control system, as they are applicable for describing risk tolerances at defined levels.
- The indicators used for setting risk tolerance of lower level objective categories can be applied to define risk appetite of the next objective category level.
Performance Measurement – COBIT 4.1

What's New
- Ericsson Improves Business Processes
- COBIT Mapping Documents
- U.S. Dept. of Veteran Affairs Transforms IT
- Government of Dubai
- COBIT Use in Korea Scoring

View All

Recognition
- Transforming Information Technology at the Department of Veterans Affairs
- COBIT Mandated for Turkish Banks
- European Commission Seeks Auditors With COBIT Experience
- COBIT Adopted by Colombian Bank Regulatory Body
- Gartner Research Note on COBIT 4.0

New COBIT 4.1 is Available!

COBIT 4.1 is an updated version of the COBIT framework, providing new guidance for IT governance. It offers a set of best practices to help organizations manage their IT investments effectively.

COBIT's success as an increasingly internationally accepted set of guidance materials for IT governance has resulted in the creation of a growing family of publications and products designed to assist in the implementation of effective IT governance throughout an enterprise.

A complimentary PDF download of COBIT 4.1 is available below. Use your existing ISACA login or register (free) when prompted to do so to download the PDF.

- [COBIT 4.1 Executive Summary and Framework](#)
- [Download COBIT 4.1](#)
- [Purchase COBIT 4.1 in print](#)
- [Access COBIT translations](#)

The following links provide additional information:

- [COBIT Online Member Discount](#): ISACA members now save 75% off the full subscription price.
- [COBIT 4.1 in Practice](#)
- [COBIT 4.1 in Action](#)
- [COBIT 4.1 in Depth](#)
- [COBIT 4.1 in Context](#)

www.ecqa.org © ecqa 2009
**Business goals**

- Maintain enterprise reputation and leadership
  - Number of incidents causing public embarrassment

**COBIT goals**

- Ensure that IT services can resist and recover from attacks
  - Number of actual IT incidents with business impact

**Process goals**

- Detect and resolve unauthorised access
  - Number of actual incidents because of unauthorised access

**Activity goals**

- Understand security requirements, vulnerabilities and threats
  - Frequency of review of the type of security events to be monitored

**Outcome measures**
Business goals

Maintain enterprise reputation and leadership

Number of incidents causing public embarrassment

COBIT IT goals

Ensure that IT services can resist and recover from attacks

Number of actual IT incidents with business impact

Process goals

Detect and resolve unauthorised access

Number of actual incidents because of unauthorised access

Activity goals

Understand security requirements, vulnerabilities and threats

Frequency of review of the type of security events to be monitored

Performance drivers

Driven by

COBIT PERFORMANCE MEASUREMENT
Maintain enterprise reputation and leadership

Ensure that IT services can resist and recover from attacks

Ensure that IT services can resist and recover from attacks

Number of actual IT incidents because of unauthorised access

Number of actual IT incidents with business impact

Number of incidents causing public embarrassment

Detect and resolve unauthorised access

Frequency of review of the type of security events to be monitored

Understand security requirements, vulnerabilities and threats

COBIT Performance Measurement

IT goals

Process goals

Activity goals

Business goals
Evidences Focusing on Objectives categories

- Assessments
  - Effectiveness goals
- Metrics
  - Efficiency goals
- Policies
  - Standardization goals
- Procedures
  - Deployment goals
- Workprograms
  - Management goals
- Workproducts
  - Documentation goals
- Activities
  - Process goals

COSO Objectives

- Strategic objectives
  - Organizational levels
- Operations objectives
  - Operational levels
- Reporting objectives
- Compliance objectives
Evidencies

Assessments
- Effectiveness goals

Metrics
- Efficiency goals

Policies
- Standardization goals

Procedures
- Deployment goals

Workprograms
- Management goals

Workproducts
- Documentation goals

Activities
- Process goals

Focusing on

Objectives categories

Strategic objectives

Operations objectives

Reporting objectives

Compliance objectives

COSO Objectives

Outcome measures

Organizational levels

Operational levels
Evidences Focusing on Objectives categories

Assessments  Effectiveness goals

Metrics  Efficiency goals

Policies  Standardization goals

Procedures  Operations objectives

Workprograms  Management goals

Workproducts  Reporting objectives

Activities  Process goals

COSO Objectives

Performance drivers
Strategic objectives

COSO OBJECTIVES

Operations objectives

Internal Control

Reporting objectives

Compliance objectives

COSO ERM

define

driven by

driven by

driven by

Level 1
Performed

Level 2
Managed

Level 3
Established

ISO/IEC 15504
CAPABILITY LEVELS

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

processes consistently enacted within defined limits

effective and efficient use of entity’s resources

defined processes used based on standard process

managed processes with established, controlled and maintained work products

reliability of reporting

compliance with applicable laws and regulations

implemented processes achieving process purpose
ISO/IEC 15504 Capability Levels

Level 0   Incomplete process
The process is not implemented or fails to achieve its purpose.

Level 1   Performed process
The process is implemented and achieves its process purpose.

Level 2   Managed process
A defined process is used based on a standard process.

Level 3   Established process
The process is managed and work products are established, controlled and maintained.

Level 4   Predictable process
The process is enacted consistently within defined limits.

Level 5   Optimizing process
The process is continuously improved to meet relevant current and projected business goals.

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

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

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

Level 5 Optimizing process
PA 5.1 Process Innovation
PA 5.2 Process Optimization
ISO/IEC 15504 Capability Levels and COSO

Level 0  Incomplete process
  The process is not implemented or fails to achieve its purpose.

Level 1  Performed process
  The process is implemented and achieves its process purpose.
  
  PA 1.1 Process Performance

Level 2  Managed process
  The process is managed and work products are established, controlled and maintained.

  PA 2.1 Performance Management
  PA 2.2 Work Product Management

Level 3  Established process
  A defined process is used based on a standard process.

  PA 3.1 Process Definition
  PA 3.2 Process Deployment

Level 4  Predictable process
  The process is enacted consistently within defined limits.

  PA 4.1 Process Measurement
  PA 4.2 Process Control

Level 5  Optimizing process
  The process is continuously improved to meet relevant current and projected business goals.

  PA 5.1 Process Innovation
  PA 5.2 Process Optimization

COSO

COMPLIANCE

STRATEGIC

OPERATIONS

RELIABLE REPORTING

www.ecqa.org © ecqa 2009
The process is not implemented or fails to achieve its purpose.

Level 0  Incomplete process

Level 1  Performed process
PA 1.1 Process Performance

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

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

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

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

The process is implemented and achieves its process purpose.

The process is enacted consistently within defined limits.

A defined process is used based on a standard process.

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

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

<table>
<thead>
<tr>
<th>ISO/IEC 15504</th>
<th>COSO</th>
<th>COBIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Category</td>
<td>Component</td>
<td>Domain</td>
</tr>
<tr>
<td>Process</td>
<td>Principle</td>
<td>Process</td>
</tr>
<tr>
<td>Process Name</td>
<td>Principle name</td>
<td>Process name</td>
</tr>
<tr>
<td>Process Purpose</td>
<td>Principle description</td>
<td>IT goal</td>
</tr>
<tr>
<td>Process Outcome</td>
<td>Attribute</td>
<td>Activity goal</td>
</tr>
<tr>
<td>Base Practice</td>
<td>Approach</td>
<td>Control Objective</td>
</tr>
<tr>
<td>Work Product</td>
<td>-</td>
<td>Input/Output</td>
</tr>
</tbody>
</table>
**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)
A two-dimensional model of Process Capability:
- Process Dimension Based on COSO Components
- Capability Dimension Based on ISO 15504-2
"The fundamental elements of a Process Reference Model are the set of descriptions of the processes within the scope of the model. These process descriptions shall meet the following requirements:

a) A process shall be described in terms of its **Purpose and Outcomes**.

b) In any description the set of process outcomes shall be **necessary and sufficient** to achieve the purpose of the process.

c) Process descriptions shall be such that **no aspects** of the measurement framework ... **beyond level 1** are contained or implied."
<table>
<thead>
<tr>
<th>Process ID</th>
<th>IFC.CE.IEV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Name</td>
<td>Integrity and Ethical Values</td>
</tr>
<tr>
<td>Process Purpose</td>
<td>Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.</td>
</tr>
<tr>
<td>Process Outcomes</td>
<td>As a result of successful implementation of IFC.CE.IEV process:</td>
</tr>
<tr>
<td></td>
<td><strong>1) Values articulated</strong> – Top management develops a clearly articulated statement of ethical values that is understood at all levels of the organization.</td>
</tr>
<tr>
<td></td>
<td><strong>2) Adherence monitored</strong> – Processes are in place to monitor adherence to principles of sound integrity and ethical values.</td>
</tr>
<tr>
<td></td>
<td><strong>3) Deviation addressed</strong> – Deviations from sound integrity and ethical values are identified in a timely manner and appropriately addressed and remedied at appropriate levels within the organisation.</td>
</tr>
<tr>
<td>Base Practices</td>
<td>IFC.CE.IEV.BP1 Articulate and Demonstrate Integrity and Ethics</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>The key members of management articulate and demonstrate the importance of sound integrity and ethical values to employees. [Outcomes: 1, 2, 3]</td>
</tr>
<tr>
<td></td>
<td>NOTE: Management can perform this practice through their:</td>
</tr>
<tr>
<td></td>
<td>• Day-to-day actions and decision-making.</td>
</tr>
<tr>
<td></td>
<td>• Interactions with suppliers, customers, and other external parties that reflect fair and honest dealings.</td>
</tr>
<tr>
<td></td>
<td>• Performance appraisals and incentives that diminish temptations inconsistent with financial reporting objectives.</td>
</tr>
<tr>
<td></td>
<td>• Intolerance of ethical violations at all levels.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>IFC.CE.IEV.BP2 Inform Employees about Integrity and Ethics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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]</td>
</tr>
</tbody>
</table>
Control over the IT process of

that satisfies the business requirement for IT of

by focusing on

is achieved by

and is measured by

Process

Purpose

Related Practices

Outcomes
ISO/IEC 15504 process assessment and the COSO frameworks
Level 1 – Compliance (Performed Process)

• The internal control process exists and provides **reasonable assurance** to the achievement of all defined outcomes complying with the relevant external and internal regulations.

• At level 1 the (financial reporting) **activities** should be investigated, whether they proof the fulfilment of purpose and existence of the outcomes of the internal financial control process contributing to the **compliance objectives of financial reporting** (activities and controls).

Compliance objectives refer to internal and external regulations or requirements. The description of internal financial control process - by the purpose statement and the outcomes - sets criteria for compliance with the relevant international control framework (COSO) and contribute to the compliance with the regulatory requirements for internal controls over financial reporting (if applicable, like SOX or Basel II).
• Besides Level 1 achievements, the internal control process is managed and provides **reasonable assurance** to the achievement of the reliable reporting objectives.

• At level 2 the (financial reporting) should be investigated, whether the **performance management and work product management indicators** related to the internal financial control process are assessable as outcome measures of the **reliability objectives of financial reporting** (activities and controls).

Management of internal financial controls might be additionally evaluated by considering other relevant sources (like Corporate Governance Codes, Audit Standards, Recommendations and Guidelines).
Level 3 – Operations (Established Process)

• Besides Level 1 and 2 achievements, the internal control process is built into the operational processes and provides **reasonable assurance** to the achievement of the objectives of “Effectiveness and efficiency of operations”.

• At level 3 the (financial reporting) activities should be investigated together with the organizational/entity level policies and procedures; whether the **process definition and process deployment indicators** are assessable as outcome measures of the **operational effectiveness and efficiency objectives** of financial reporting (at corporate levels).

  Standardization is necessary for supporting measurement of operational effectiveness and efficiency, when evaluation is based on predefined comparable information.

The internal financial control process will better support the achievement of effectiveness and efficiency goals of operational units (effecting financial reporting objectives), if its design is based on Policies and Procedures consistent with the corporate structure and the entity’s risk appetite.
• Besides Level 1, 2 and 3 achievements, the internal control process is incorporated into the enterprise risk management system and provides **reasonable assurance** to the achievement of the Strategic objectives relating to high-level goals, aligned with and supporting the entity’s mission.

• At level 4 the **key controls** should be investigated as an entity level key control (how applied in strategy setting and across the enterprise) within the entity level risk management, whether the **process measurement and process control indicators** are assessable as outcome measures of assurance regarding the **entity’s strategic objectives** of financial reporting.

  Key controls are those significant controls within business processes, which if operating correctly will both ensure and give assurance that the organization is achieving its key business objectives. Effectiveness judgment of key controls assumes process measurement directly linked to enterprise objectives.
COSO & COBIT Process Assessment

Measurement Framework

COSO Objective Categories
- Strategic
  - high-level goals, aligned with and supporting entity’s mission
- Operations
  - effective and efficient use of entity’s resources
- Reporting
  - reliability of reporting
- Compliance
  - compliance with applicable laws and regulations

COBIT Performance Drivers
- Strategic Goals
  - driven by the outcome measures of Established IT processes
- Effective and efficient business operation
  - driven by the outcome measures of Managed IT Processes
- Reliable IT operation
  - driven by the outcome measures of Performed IT Processes
- IT Goals
  - driven by the outcome measures of IT Activities

GOVERNANCE

SPICE

20 Control Processes
34 ITGC Processes

Process Reference Models

Financial Reporting Activities

Business Processes

Supervision & Management

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

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.

Risk Tolerance

Risk Appetite

COSO & COBIT Process Assessment

48
Control Risk Assessment

Target and Assessed Attributes

Process

<table>
<thead>
<tr>
<th>Process</th>
<th>Process Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Performed</td>
</tr>
<tr>
<td>IFC.CE.VEV</td>
<td>F</td>
</tr>
<tr>
<td>Integrity and Ethical Values</td>
<td>F</td>
</tr>
<tr>
<td>IFC.RA.FRO</td>
<td>F</td>
</tr>
<tr>
<td>Financial Reporting Objectives</td>
<td>F</td>
</tr>
<tr>
<td>IFC.CA.PP</td>
<td>F</td>
</tr>
<tr>
<td>Policies and Procedures</td>
<td>F</td>
</tr>
<tr>
<td>IFC.IC.IC</td>
<td>F</td>
</tr>
<tr>
<td>Internal Communication</td>
<td>F</td>
</tr>
<tr>
<td>IFC.MO.PD</td>
<td>F</td>
</tr>
<tr>
<td>Reporting Deficiencies</td>
<td></td>
</tr>
</tbody>
</table>
• „None”
• „Minor” – one-step gap in case of “Fully achieved” attribute target.
• „Major” – two or more steps distance deems major gap in case of “Fully achieved” attribute target. At “Largely achieved” target even the one step distance (“Partially achieved”) means major gap.
Control Risk Assessment
Capability Level Gaps

The process related risk depends on both the probability of problem arising from the identified gap and the potential consequence. In general the consequences depend on the capability levels where the gaps occur:

- None - No major or minor gaps
- Slight - No gap at Level 1, and only minor gaps at higher levels
- Significant - A minor gap at Level 1, or a single major gap above
- Substantial above - A major gap at Level 1, or more than one major gap
## Control Risk Assessment

**ISO/IEC 15504 based Risk Map**

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Slight</td>
</tr>
<tr>
<td>Indicated by capability level where gap occurs</td>
<td></td>
</tr>
<tr>
<td>5 – Optimizing</td>
<td>Low Risk</td>
</tr>
<tr>
<td>4 - Predictable</td>
<td>Low Risk</td>
</tr>
<tr>
<td>3 - Established</td>
<td>Low Risk</td>
</tr>
<tr>
<td>2 - Managed</td>
<td>Medium Risk</td>
</tr>
<tr>
<td>1 - Performed</td>
<td>Medium Risk</td>
</tr>
</tbody>
</table>
### IFC.RA.FRO - Financial Reporting Objectives

<table>
<thead>
<tr>
<th>Target profile</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA 1.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PA 2.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
</tr>
<tr>
<td>PA 2.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
</tr>
<tr>
<td>PA 3.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
</tr>
<tr>
<td>PA 3.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
</tr>
<tr>
<td>PA 4.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
</tr>
<tr>
<td>PA 4.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
</tr>
</tbody>
</table>

- Target profile gap: minor
- Capability level gap: slight
- Capability level risk: low
- Process related risk: low

### IFC.CA.PP - Policies and Procedures

<table>
<thead>
<tr>
<th>Target profile</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA 1.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PA 2.1</td>
<td>F</td>
<td>P</td>
<td>L</td>
<td>F</td>
</tr>
<tr>
<td>PA 2.2</td>
<td>F</td>
<td>P</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>PA 3.1</td>
<td>F</td>
<td>P</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>PA 3.2</td>
<td>F</td>
<td>P</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>PA 4.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
</tr>
<tr>
<td>PA 4.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>L</td>
</tr>
</tbody>
</table>

- Process attribute gap: major, minor
- Capability level gap: significant
- Capability level risk: medium
- Process related risk: medium

### IFC.IC.IC - Internal Communication

<table>
<thead>
<tr>
<th>Target profile</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA 1.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PA 2.1</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>F</td>
</tr>
<tr>
<td>PA 2.2</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>F</td>
</tr>
<tr>
<td>PA 3.1</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>F</td>
</tr>
<tr>
<td>PA 3.2</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>F</td>
</tr>
<tr>
<td>PA 4.1</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>F</td>
</tr>
<tr>
<td>PA 4.2</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>F</td>
</tr>
</tbody>
</table>

- Process attribute gap: major, major, major
- Capability level gap: substantial, substantial
- Capability level risk: high, high
- Process related risk: high
Control Deficiencies

- **Control Deficiency**: controls are not in place, or inadequate, or not being used
- **Significant Deficiency**: Deficiency in a significant control, or aggregation of deficiencies that could result consequential impact
- **Material Weakness**: Significant deficiency or an aggregation of significant deficiencies that preclude the entity’s internal control from providing reasonable assurance that material misstatements or any major ”loss” will be prevented or detected on a timely basis by employees **in the normal course** of performing their assigned functions
“... evaluating deficiencies and whether they constitute significant deficiencies or material weaknesses will necessarily always involve judgment.”

– PCAOB

Risk appetite
Effectiveness Conclusion on Design and Operation of Internal Controls

• The Process Assessment Profiles are used for making opinion about the effectiveness of control design, namely in what extent the design of controls meets the organizational risk appetite represented by the target control process capability profiles.

• Additionally the ISO/IEC 15504-4 based Control Risk Assessment provides practical tool for judgement about the effectiveness of control operation, whether the assessed process capability profiles constitute reasonable assurance concerning achievement of related business objectives, such as the low control process related risk levels represent remote likelihood that material weaknesses will not be prevented or detected on a timely basis.
• Providing **Assessment Model** for internal controls by using the COSO & COBIT based Process Reference Models.
• Offering tools for internal control risk assessment supporting the communication of **internal control weaknesses** and the considerations of necessary corrective actions.
• Focusing on specific and generic **assessment indicators** applicable for compliance, reliable reporting, operational effectiveness and strategic objectives.
• Applying assessment indicators for collecting evidences from **business activities** and **entity/corporate levels**, as well.
• Differentiating “internal controls” as a **system** from the underlying “control activities” as the object of monitoring.
• Linking **operational effectiveness** considerations of business processes to the achievement of internal control objectives.
• Organizational maturity is the extent to which an organization consistently implements processes within a defined scope – derived from the specified Process Assessment Model(s) - that contributes to the achievement of its business goals.

• The new part of the ISO/IEC 15504 standard defines a measurement framework for the assessment of organizational maturity.

• Within this measurement framework, each level of organizational maturity is characterised by the demonstration of achievement of specified levels of process capability in process sets drawn from the specified Process Assessment Model(s).

• Predictable (Level 4) organizational maturity: all processes assigned to Maturity Levels 1, 2, 3, and 4 shall achieve process Capability Level 3 or higher. One or more of the processes in the basic process set shall achieve process Capability Level 4 or higher.
“Key controls are those significant controls within our business processes, which if operating correctly will both ensure and give assurance that the organization is achieving its key business objectives.”

Key controls are either selected control processes from the Process Reference Model(s) or a subset of the relevant business processes operating at entity or even activity levels, with which the basic process set of the assessment model is necessarily completed.

The key control processes - defined based on the ISO/IEC 15504-2 requirements - can be added to the basic process set for the organizational maturity model (ensuring the achievement of level 1 (basic) maturity).

The basic process set should include a minimum set of key control processes, together with additional and optional processes determined by the organizational context for the assessment.
COSO processes formulating extended process sets

- Implementing a comprehensive set of internal financial control processes from the **COSO based Process Reference Model** contributes to the achievement of all process attributes up to level 4 at an entity level key control.

- The process performance indicators, such as *base practices* and *work products* of the supporting internal financial control processes provide persuasive information for **capability level 4 assessment** of the key control processes (from the basic process set).

- By this approach the 20 internal financial control processes derived from the Principles of the COSO 2006 Guidance can be used to formulate the **extended process sets** for the organizational maturity model ensuring the achievement of the level 2 (*managed*) and level 3 (*established*) maturity.
Developing and assessing the necessary and sufficient key controls (as part of the basic process set) should follow **risk-based and top-down approach**.

Effective design and operation of the internal control system presume that **all risks, which can have material (more than significant) effect on business objectives, are responded in a cost effective way**, so the applied set of key controls ensures that the probability of a material deviation from objectives (like misstatement in financial report) is remote or the consequence of a control deficiency (even considered its cumulative effect) remains within tolerable limits.
• The key controls are operating at entity, intermediate or activity levels, and can have either direct or indirect relationship to the **risk of material error**.

• The **outcomes of the 20 internal financial control processes** of the COSO based Process Reference Model (as part of the extended process sets) provide evidences that key controls are designed by applying risk management and internal control principles and also support that **key controls are operating at level 4 (predictable) capability**.

• Furthermore, some of the 20 internal financial control processes can be also implemented as **entity-level key controls** based on circumstances.
Topics covered

- "Governance" SPICE
- COSO Frameworks
- Setting Objectives in Enterprise Risk Management
- COBIT Performance Measurement
- COSO Objective Categories
- COSO-SPICE Performance Measurement
- Mapping COSO Objectives with Capability Levels
- COSO & COBIT as Process Reference Models
- Control Risk Assessment
- Effectiveness Conclusion on Design and Operation of Internal Controls by using Process Assessment Results
- Key Controls: Applying Organizational Maturity concept

Thank you for your attention!

János Ivanyos
ivanyos@memolux.hu, www.training.ia-manager.org
European Internal Financial Control Assessor Training and Certification Programme

Assessing Internal Financial Control Systems

Available course resources: English, Hungarian, Spanish, Romanian, German, Slovak

The key objective of this training programme supported by the European Commission is setting up a modular structure of internal controls for financial reporting, which is commonly applicable in each sector under related regulatory directives (like financial regulation of using EU, national and other public funds; Basel II for bank sector; SOX or EU Company Law for listed companies, etc.). This modular structure is the base for applying standard evaluation method. The features of internal financial control processes and the process assessment method can be acquired by taking the training course containing online and traditional learning elements. A modular certificate can be achieved by passing online exam based on the European skills card definition of the necessary professional requirements.

The COSO internal control framework and the ISO/IEC 15504 (SPICE) process assessment methodology were used for the development of the skill card and the related training materials of the “Certified European Internal Financial Control Assessor” programme including adaptation of the Principles, Attributes and Approaches of the COSO 2006 Guidance as agreed with the COSO Board for Spanish, German, Romanian, Slovak and Hungarian translations. The core document of the COSO-based Process Reference Model and Process Performance Indicators is under Copyright © 2006 by The Committee of Sponsoring Organization (COSO). All rights reserved.

© COSO SPICE (ISO/IEC 15504 conformati) Reference