Applying Integrated Risk Management
Scenarios for Better Controls at SMEs

János Ivanyos
Budapest Business School
ivanyos@trusted.hu
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
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
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

COSO 2006
- 20 Control Processes

COBIT 4.1
- 34 ITGC Processes

Governance SPICE: Capability Measures for Assurance and Improvement

- Measurement Framework
  - COSO Objective Categories
  - COBIT Performance Drivers

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

Predictable
- The process is enacted consistently within defined limits.

Operations
- Effective and efficient use of entity's resources

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

Performing
- The process is implemented and achieves its process purpose.

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

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

Optimizing
Quantitative measures are implemented to continuously improve the process

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

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

Managed
Processes and work products are managed, responsibilities are identified

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

Incomplete
Chaotic processes

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

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
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

ISO/IEC 15504-2

COSO

Process Reference Model

PROCESS Dimension

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

<table>
<thead>
<tr>
<th></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>F</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: F
- Assessed profile: F
- Process attribute gap: -
- Capability level gap: slight
- Capability level risk: low
- Process related risk: low

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

<table>
<thead>
<tr>
<th></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>-</td>
</tr>
<tr>
<td>PA 2.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 2.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 3.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 3.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 4.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 4.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
</tbody>
</table>

- Target profile: F
- Assessed profile: F
- 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></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>-</td>
</tr>
<tr>
<td>PA 2.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 2.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 3.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 3.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 4.1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
<tr>
<td>PA 4.2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>-</td>
</tr>
</tbody>
</table>

- Target profile: F
- Assessed profile: P major N major N
- Process attribute gap: subst. substantial subst. -
- Capability level gap: subst. substantial substant.
- Capability level risk: high high medium
- Process related risk: high
COSO model applicability

• Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control—Integrated Framework, 1992
• Basle Committee on Banking Supervision: Framework for Internal Control Systems in Banking Organisations, 1998
• INTOSAI: Guidelines for Internal Control Standards for the Public Sector, 2004
• COSO Enterprise Risk Management—Integrated Framework, 2004
• COSO Small Business Guidance, 2006
• COSO 2013
• SOX (US), Company Law in the EU, Corporate Governance Codes, etc.
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

Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3891, USA. All rights reserved.

Permission has been obtained from the copyright holder, The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3891, U.S.A., to publish this translation, which is the same in all material respects, as the original, unless approved as changed. Permission has been obtained to publish this translation in the following publication: European Internal Financial Control Assessor. No part of this document may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of The Committee of Sponsoring Organizations of the Treadway Commission.
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 remediated at appropriate levels within the company.
### Table 1: Process Performance Indicators: Integrity and Ethical Values (IFC.CE.IEV)

<table>
<thead>
<tr>
<th>Process ID</th>
<th>IFC.CE.IEV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Name</strong></td>
<td>Integrity and Ethical Values</td>
</tr>
<tr>
<td><strong>Process Purpose</strong></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><strong>Process Outcomes</strong></td>
<td>As a result of successful implementation of IFC.CE.IEV process:</td>
</tr>
<tr>
<td></td>
<td>1) <strong>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>2) <strong>Adherence monitored</strong> – Processes are in place to monitor adherence to principles of sound integrity and ethical values.</td>
</tr>
<tr>
<td></td>
<td>3) <strong>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>
</tbody>
</table>
Tabuľka 1: Ukazovatele výkonu procesu: Integrita a etické hodnoty (IFC.CE.IEV)

<table>
<thead>
<tr>
<th>Identifikátor procesu</th>
<th>IFC.CE.IEV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Názov procesu</td>
<td>Integrita a etické hodnoty</td>
</tr>
<tr>
<td>Účel procesu</td>
<td>Rozvíja sa dôkladná integrita a etické hodnoty, najmä vrcholového manažmentu, a ich chápanie a určujú štandard správania pri finančnom vykazovaní.</td>
</tr>
<tr>
<td>Výstupy procesu</td>
<td>Výsledkom úspešnej implementácie procesu IFC.CE.IEV sú:</td>
</tr>
<tr>
<td></td>
<td>1) Jasné hodnoty – Vrcholový manažment vytvára jasne formulované stanovisko ohľadom etických hodnôt, ktoré je pochopené na všetkých úrovniach organizácie.</td>
</tr>
<tr>
<td></td>
<td>2) Monitorované dodržiavanie – Sú zavedené procesy na monitorovanie dodržiavania zásad dôslednej integrity a etických hodnôt.</td>
</tr>
<tr>
<td></td>
<td>3) Vysporiadanie sa s odchýlami – Odchýlky od dôkladnej integrity a etických hodnôt sa včas identifikujú a na ich odstánenie sa na príslušných úrovniach v rámci podniku prijímanú opravné prostriedky.</td>
</tr>
</tbody>
</table>
**COSO 2006 Guidance – Level 1 Indicators**

**Applying Integrated Risk Management Scenarios for Better Controls at SMEs**

**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.

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.

**Base Practice**
<table>
<thead>
<tr>
<th>Base Practices</th>
<th>IFC.CE.IEV.BP1 Articulate and Demonstrate Integrity and Ethics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The key members of management articulate and demonstrate the</td>
</tr>
<tr>
<td></td>
<td>importance of sound integrity and ethical values to employees.</td>
</tr>
<tr>
<td></td>
<td>[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</td>
</tr>
<tr>
<td></td>
<td>parties that reflect fair and honest dealings.</td>
</tr>
<tr>
<td></td>
<td>• Performance appraisals and incentives that diminish</td>
</tr>
<tr>
<td></td>
<td>temptations inconsistent with financial reporting</td>
</tr>
<tr>
<td></td>
<td>objectives.</td>
</tr>
<tr>
<td></td>
<td>• Intolerance of ethical violations at all levels.</td>
</tr>
<tr>
<td></td>
<td>IFC.CE.IEV.BP2 Inform Employees about Integrity and Ethics</td>
</tr>
<tr>
<td></td>
<td>Management implements mechanisms to inform new employees and</td>
</tr>
<tr>
<td></td>
<td>remind current personnel of the organisation’s objectives</td>
</tr>
<tr>
<td></td>
<td>related to integrity and ethics and related corporate</td>
</tr>
<tr>
<td></td>
<td>values.</td>
</tr>
<tr>
<td></td>
<td>[Outcomes: 1, 2]</td>
</tr>
<tr>
<td>Inputs</td>
<td>Outputs</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Code of Conduct [Outcome: 1]</td>
</tr>
<tr>
<td></td>
<td>Monitoring Reports [Outcome: 2]</td>
</tr>
<tr>
<td>Periodic Staff Information [Outcomes: 1, 2, 3]</td>
<td>Periodic Staff Information [Outcomes: 1, 2, 3]</td>
</tr>
</tbody>
</table>

**Work Products**
Internal Financial Control Assessor Skillcard

Applying Integrated Risk Management Scenarios for Better Controls at SMEs

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
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
Applying Integrated Risk Management Scenarios for Better Controls at SMEs

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

of Internal Financial Control Assessor

---

**ECQA certified Internal Financial Control Assessor**

---

**Legend**

- **SCIA:** General Environment
  - Integrity and Ethical Values (E1)
  - Oversight Board (E2)
  - Management's Philosophy and Operating Role (E3)
  - Organizational Structure (E4)
  - Financial Reporting Compromises (E5)
  - Accountability and Transparency (E6)
  - Risk Management (E7)

- **SCIA:** Risk Assessment
  - Financial Reporting Objectives (E1)
  - Financial Reporting Risk (E2)
  - Fiscal Risk (E3)

- **SCIA:** Control Activity
  - Integration with Risk management (E1)
  - Policy and Procedures (E2)
  - Information Technology (E3)

- **SCIA:** Information and Communications
  - Financial Reporting Information (E1)
  - Internal Control Information (E2)
  - External Communication (E3)

- **SCIA:** Monitoring
  - Ongoing and Reporting Findings (E1)
  - Reporting Information (E2)

---

**MONTIFIC - Multilingual ONTology for Internal Financial Control**
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

Applying Integrated Risk Management Scenarios for Better Controls at SMEs

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.

Risk Management’s Role in Corporate Governance

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**
- Mandate & Commitment
- Design framework for managing risk
- Continually improve the framework
- Implement risk management
- Monitor and review the framework

**RM Process**
- Establish the context
- Risk assessment
  - Risk identification
  - Risk analysis
  - Risk evaluation
- Risk treatment
- Communicate and consult
- Monitor and review

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

Applying Integrated Risk Management Scenarios for Better Controls at SMEs
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)

SUSTAINABLE BUSINESS OPERATION

COMPETITIVENESS
- 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

STAKEHOLDERS’ EXPECTATIONS

BUSINESS ENVIRONMENT

HARBIF International Workshop, Budapest Business School, Budapest, Hungary, 4 April 2014
Enabling Processes and Practices for Capable Business Operation

- Stakeholders’ Expectations
- Capable Business Operation
  - Commitment
    - COSO IFC.CE.IEV Integrity and Ethical Values
    - COBIT PQ2 Ensure Continuous Service
    - COSO IFC.CE.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

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

STAKEHOLDERS’ EXPECTATIONS

CONTROL EFFICIENCY

BUSINESS ENVIRONMENT
Applying Integrated Risk Management Scenarios for Better Controls at SMEs
Governance Level 1: Performed Business Operation
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.
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

Diagram:
- Managing Operational Risks
- Managing Operational Effectiveness
- Managing Performance Reliability
- Managing Strategic Directions
- Managing Operational Performance

Applying Integrated Risk Management Scenarios for Better Controls at SMEs
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

Diagram showing the flow of managing operational risks, operational effectiveness, strategic directions, performance reliability, and operational performance.
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

Applying Integrated Risk Management Scenarios for Better Controls at SMEs
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 Operational Risks
- Managing Operational Effectiveness
- Managing Performance: Reliability
- Managing Strategic Directions
- Managing Operational Performance

Diagram showing the flow between managing operational risks, operational effectiveness, performance reliability, strategic directions, and operational performance.
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.
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
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!