Governance Model for Trusted Businesses

Linking Governance to Sustainable Value Creation

Deliverable of the

Business Process Modelling for Governance SPICE and Internal Financial Control

BPM GOSPEL

Project

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

File: Governance SPICE Model v24

Contents

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. Introduction

1.1 Objective

The objective of this material is providing governance objectives based process descriptions with practices as special application areas of Enterprise Governance by using COSO [1], COBIT [2] and Enterprise SPICE [3] models in a format, which is conformant with the ISO/IEC 15504 Process Assessment standard (currently transitioning to ISO/IEC 33001-99) [4] and applicable for management assertions and audit reports on design and operation effectiveness of internal controls over financial reporting and for providing assurance of trusted and sustainable business operation.

1.2 Purpose of the material

This material will be used as training and knowledge-sharing resource being exploited by the BPM GOSPEL project consortium members available via public internet site (www.governancecapability.com) for governance system implementation, concerning skill self-assessment and process assessment exercises.

1.3 The BPM GOSPEL project

The objective of the BPM GOSPEL - Business Process Modelling for Governance SPICE and Internal Financial Control - project (2010-2012) is the transfer of the already proved innovation from Germany to Hungary, where the existing results of IA-Manager (2005-2007) and MONTIFIC (2008-2010) training development projects are further enriched by the adapted "Stages" process management platform (see: www.methodpark.com/en/product.html) for multi-layer Business Process Modelling (BPM). The project aims to provide ready to use scenarios for enterprises and best practice cases for teaching and learning in vocational trainings demanded by both sides of the labour market.

Implemented BPM layers are presented below:

Figure 1: Implemented layers for Business Process Modelling (BPM GOSPEL)

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

This Governance Model - as a key conceptual deliverable of the BPM GOSPEL project - provides reference processes for mapping operational management to compliance and audit management implemented by “Stages” platform. The best practice case studies aim to present all the above layers in different instances.

Adding business driven case studies into training programmes (like www.training.ia-manager.org) supports understanding the competencies needed and best practices relevant for business practitioners. Employers are interested in on-the-job trainings where the acquired skills and knowledge can be directly tested and certified by applying the offered methodology and tools in live environment.

The platform system "Stages" is adapted as a multi-layer BPM master example for teaching and even "coaching" practical implementation of internal financial controls with IT support applied by private and public sector companies following internationally recognized control frameworks like COSO and COBIT, and related assessment (audit) approach (Governance SPICE).

The BPM GOSPEL Project Partnership

Prime Contractor: Budapest Business School
Country: HU-Hungary
Homepage: www.bgf.hu

Contact Persons
József ROÓZ, rector emeritus
László VARGA, project manager
Address: Markó utca 29-31, H-1055 Budapest
Telephone: +36 1 301 3427
Fax: +36 1 301 3431
E-mail: varga.laszlo@bgf.hu

Project Coordinator: Memolux Ltd.
Country: HU-Hungary
Homepage: www.memolux.hu

Contact Person
Name: János IVANYOS
Address: Erzsébet királyné útja 125, H-1142 Budapest
Telephone: +36 2 0941 7075
E-mail: ivanyos@trusted.hu

Partners:
Gemma Ltd.
Country: HU-Hungary
Homepage: www.gemma.hu

Method Park Software AG
Country: DE-Germany
Homepage: www.methodpark.de

International Software Consulting Network - ISCN Ltd.
Country: IE-Ireland
Homepage: www.iscn.com

See more details at: www.ia-manager.org and
http://www.adam-europe.eu/adam/project/view.htm?prj=6635

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1.4 References

[1] Internal Control over Financial Reporting — Guidance for Smaller Public Companies
Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved.

[2] Control Objectives for Information and related Technology - COBIT® 4.1
Copyright © 2007 by the IT Governance Institute. 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA. All rights reserved.

[3] Enterprise SPICE® - An Integrated Model for Enterprise-wide Assessment and Improvement
Technical Report – Issue 1 September 2010
Copyright © The SPICE User Group 2010.

[4] ISO/IEC 15504-1:2004 Information technology -- Process assessment -- Part 1: Concepts and vocabulary
ISO/IEC 15504-2:2003 Information technology -- Process assessment -- Part 2: Performing an assessment
ISO/IEC 15504-2:2003/Cor 1:2004
ISO/IEC 15504-3:2004 Information technology -- Process assessment -- Part 3: Guidance on performing an assessment
ISO/IEC 15504-4:2004 Information technology -- Process assessment -- Part 4: Guidance on use for process improvement and process capability determination

[5] J. Ivanyos, J. Roóz and R. Messnarz, Governance Capability Assessment: Using ISO/IEC 15504 for Internal Financial Controls and IT Management, in: The MONTIFIC Book, MONTIFIC-ECQA Joint Conference Proceedings, 2010

[6] Trust Services Principles, Criteria, and Illustrations
Copyright © 2009 by the American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants.

[7] Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization
Copyright © 2010 American Institute of Certified Public Accountants, Inc. New York, NY 10036-8775

[8] Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)
Copyright © 2011, American Institute of Certified Public Accountants, Inc. All Rights Reserved.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2. Governance Objectives for Trusted Businesses

2.1 Using Governance Capability Assessment (Governance SPICE)

The term of "Governance Capability Assessment" [5] is used in context of Governance, Risk Management and Internal Control processes based on different concepts:

- Corporate Governance Principles (OECD)
- Recognized Control Frameworks and Reference Models (like COSO, COBIT, Enterprise SPICE, etc.)
- Risk Tolerance and Risk Appetite (as of COSO ERM)
- Performance Measurement (as of COBIT)
- Process Capability Assessment (ISO/IEC 15504-2:2003)
- Evaluating Process-related Risk (ISO/IEC 15504-4:2004)
- Organizational Maturity (ISO/IEC TR 15504-7:2008)

"Governance Capability" is the COSO objective-category based characterization of the ability of a process to meet current or projected business goals:

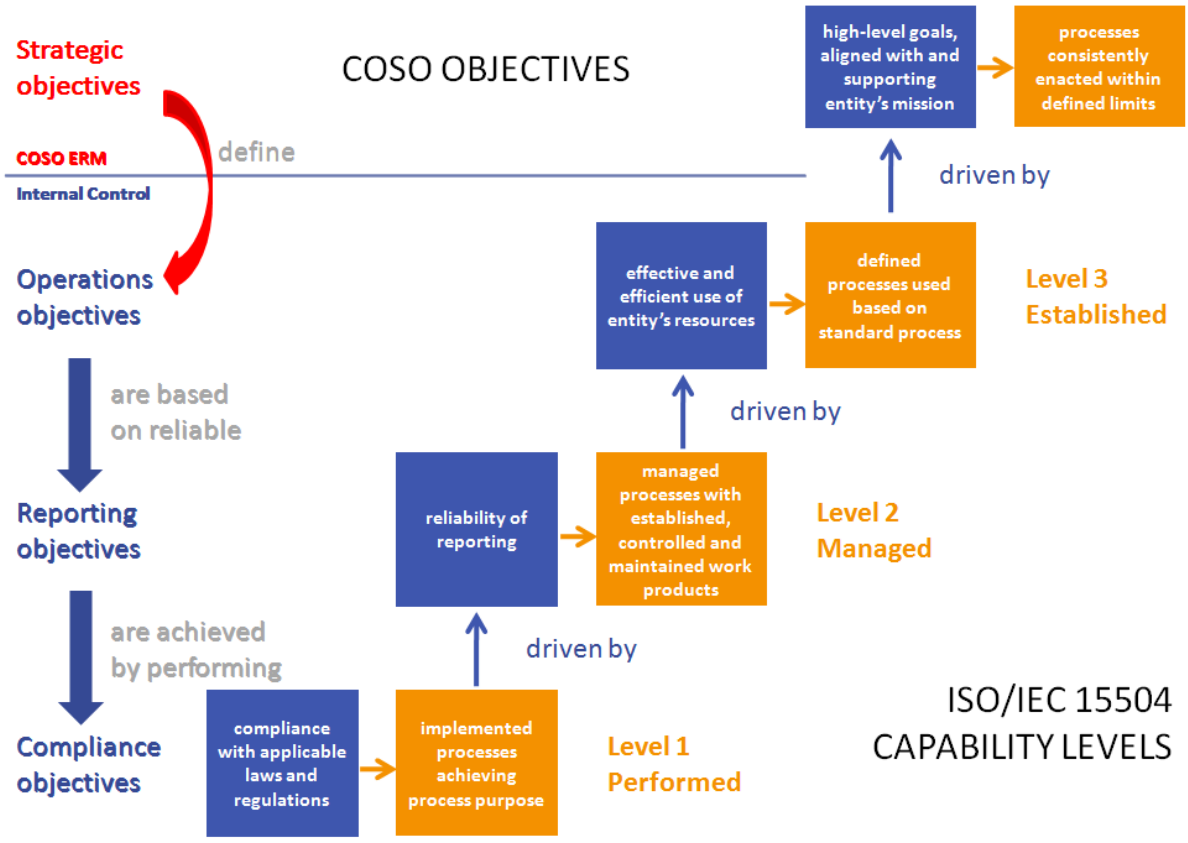

Figure 2: Implementing Governance Capability Levels

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Internal and external audit standards (like IIA and ISA) recommend system based evaluation of existing internal controls against internationally recognized control frameworks like COSO (Internal Control – Integrated Framework) and COBIT (Control Objectives for Information and related Technology). The contents of these frameworks are applicable to set up Process Reference Models in compliance with ISO/IEC 15504-2 requirements.

Figure 3 presents the general concept of how the ISO/15504 capability measurement is applicable for assessing governance systems implementing the most acknowledged control frameworks such as COSO and COBIT. The presented 3 dimensions are those derived from the COSO enterprise risk management and internal control models:

- Management supervision and control of business processes and activities
- Governance processes supporting the design and operation of internal control system
- Objective categories measuring achievement of entity-level and operational goals

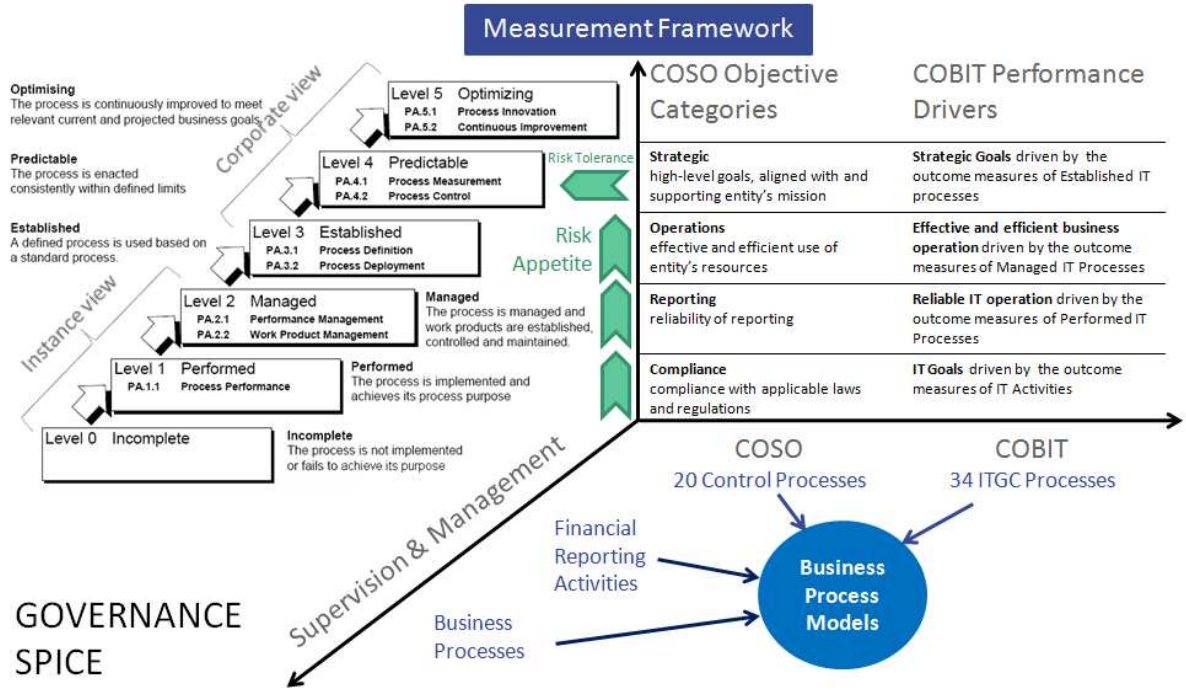

Figure 3: Governance SPICE Model

The COSO and COBIT based Process Reference Models associated with the process attributes defined in ISO/IEC 15504-2 provide a common basis for performing assessments of governance capability regarding internal controls and reporting of results by using a common rating scale. ISO/IEC 15504 offers not only transparent method for assessing performance of relevant governance processes, but also tools for assessing control risk areas based on the gaps between target and assessed capability profiles.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.2 Scope of the Governance Objectives

The well established and recognized control frameworks and process reference models 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 enterprise 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.

The Governance 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.

The reference to applicable ISO/IEC 15504 conformant processes allows management and auditors to use governance capability profiles in context of the governance objectives.

The Governance Model interprets the following governance objectives for determining governance processes as special applications of the recognized reference models (COSO, COBIT and Enterprise SPICE) and trusted business principles [6]:

- Supporting Organization's Internal Control System
  - Risk Awareness
  - Accountability
  - Competency
  - Accuracy
  - Process Integrity
  - Data Protection
  - Commitment
  - Control Efficiency

- Supporting Business Sustainability
  - Competitiveness
  - Exploitability
  - Satisfaction

Governance Capability Levels and related Process Attributes for processes supporting the above objectives as application practices can be applied as qualitative and quantitative measures for setting affordable enterprise specific requirements (risk appetite) relevant for achieving the business goals within a tolerable deviation (risk tolerance).

The Governance Model provides descriptions and application practices of governance processes for management assertions and audit reports on design and operation effectiveness of internal controls over financial reporting and for providing assurance of trusted and sustainable business operation.

For rationale of the Governance Model structure, the following parts present the governance objectives by determining the concerning key risks and risk factors. The risk responses should be decided by the enterprise management as adequate applications of the referred (COSO, COBIT and Enterprise SPICE) processes at the defined governance capability levels.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3 Setting Governance Objectives for Controlled Business Operation

2.3.1 Risk Awareness

Key Risk	Risk Factors	Responses	Applicable COSO processes	Application Practices
Relevant governance risks are not considered	Governance objectives for business processes are inadequately established	Management sets clearly defined objectives for governance including risk tolerance and risk appetite	Governance (Financial Reporting) Objectives (COSO)	Management specifies governance objectives relevant for financial reporting and trusted business operation with sufficient clarity and criteria to enable the identification of risks to the achievement of the governance objectives relevant for financial reporting and trusted business operation.
	Inconsistency in risk assessment	Risk assessments are periodically performed by considering the time horizon of the governance objectives, risk tolerance and risk appetite	Governance (Financial Reporting) Risks (COSO)	The organization identifies and analyses risks to the achievement of governance objectives relevant for the organization's financial reporting and trusted business operation as a basis for determining how the risks should be managed.
	Risks relevant for organizations' internal control system are not addressed	Control activities developed by reflecting to all assertions relevant for organization's internal control system	Integration with Risk Assessment (COSO)	Actions are taken to address risks to the achievement of governance objectives relevant for financial reporting and trusted business operation.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3.2 Accountability

Key Risk	Risk Factors	Responses	Applicable COSO processes	Application Practices
Management is unable to control business processes	No consistent or properly communicated policies and procedures	Policies and procedures are maintained and used in operation	Policies and Procedures (COSO)	Governance policies related to reliable financial reporting and trusted business operation are established and communicated throughout the organisation, with corresponding procedures resulting in management directives being carried out.
	Management structure is inadequate	Roles and responsibilities are identified	Authority and Responsibility (COSO)	Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting and trusted business operation.
	Management attitude is not exemplary	Management takes stimulating behaviour	Management's Philosophy and Operating Style (COSO)	Management's philosophy and operating style support achieving effective internal control over financial reporting and trusted business operation.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3.3 Competency

Key Risk	Risk Factors	Responses	Applicable COSO processes	Application Practices
Staff is unable to perform control tasks	Lack of skilled staff	Recruitment, compensation and training activities are performed systematically	Human Resources (COSO)	Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting and trusted business operation.
	Staff members do not know procedures and processing requirements	Staff members are continually informed, feedbacks are periodically reviewed	Internal Communication (COSO)	Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.
	Changes of Skills Requirements	Adequate human resource practices are determined and used	Governance (Financial Reporting) Competencies (COSO)	The organization retains individuals competent in relation to the organization's business operation, financial reporting and related oversight roles.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3.4 Accuracy

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

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3.5 Process Integrity

Key Risk	Risk Factors	Responses	Applicable COSO processes	Application Practices
Defective process level controls	Process performance is wholly dependent on key staff	Control activities over access, amendments, adjustments and other usage of business information are maintained systematically	Selection and Development of Control Activities (COSO)	Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting and trusted business operation objectives.
	Data processing and process automation controls malfunction	Application and general IT controls are maintained and evaluated systematically	Information Technology (COSO)	Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting and trusted business operation objectives.
	Failures of detecting errors and reacting to incidents	Process performance metrics are collected and evaluated	Ongoing and Separate Evaluations (COSO)	Ongoing and/or separate evaluations enable management to determine whether internal control over financial reporting and trusted business operation is present and functioning.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3.6 Data Protection

Key Risk	Risk Factors	Responses	Applicable COSO&COBIT processes and GAPP	Application Practices
Unauthorized access to and misuse of confidential data	System security and confidentiality failures	Preventive controls maintained to avoid system security incidents	Ensure Systems Security (COBIT)	Satisfy the business requirement of maintaining the confidentiality, integrity and availability of information and the processing infrastructure aligned to business needs and minimising the impact of security vulnerabilities.
	Intentional misuse of data	Anti-fraud management program maintained	Fraud Risks (COSO)	The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting and trusted business operation objectives.
	Breaching privacy requirements	Active policies and procedures are in place to ensure privacy requirements	Generally Accepted Privacy Principles (AICPA/CICA)	Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP).

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3.7 Commitment

Key Risk	Risk Factors	Responses	Applicable COSO&COBIT processes	Application Practices
Business integrity is not respectable	No commitment to ethical values	Ethical values are articulated and followed	Integrity and Ethical Values (COSO)	Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting and trusted business operation.
	Interruption of information and communication systems	Active policies and procedures are in place to ensure business continuity	Ensure Continuous Service (COBIT)	Satisfy the business requirement of ensuring minimal business impact in the event of an IT service interruption.
	External feedbacks and opinions are not considered	Information from external parties are collected and reviewed systematically	External Communication (COSO)	Matters affecting the achievement of the financial reporting and trusted business operation objectives are communicated with outside parties.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.3.8 Control Efficiency

Key Risk	Risk Factors	Responses	Applicable COSO processes	Application Practices
Inefficient usage of control resources	Inadequate structures for control operation and reporting	Management maintains adequate organizational structure and reporting lines	Organizational Structure (COSO)	The entity's organizational structure supports effective internal control over financial reporting and trusted business operation.
	Operation and reporting of controls don't provide sufficient evidences to assess effectiveness of the internal control system	Oversight activities ensure periodic assessment on governance capabilities	Oversight Board (COSO)	The oversight board understands and exercises oversight responsibility related to trusted business operation, financial reporting and related internal control.
	Necessary corrective actions are not taken in time	Management reviews control deficiencies and actions taken	Reporting Deficiencies (COSO)	Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to the management and the oversight board as appropriate.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.4 Setting Governance Objectives for Sustainable Business Operation

2.4.1 Competitiveness

Key Risk	Risk Factors	Responses	Applicable Enterprise SPICE processes	Application Practices
Loosing market	Business objectives are not reflecting to the changes of economic environment	Business goals and targets are systematically maintained	Enterprise Governance (ESPICE)	The organization applies practices to establish strategic enterprise direction and ensure the enterprise achieves its goals and objectives.
	Market needs are not respected	Improvement of product or service features are considered periodically	Needs (ESPICE)	The organization applies practices to elicit, analyze, clarify, and document evolving customer and other stakeholder needs and expectations.
	Business proposals are not convincing	Improvement of proposal preparation	Tendering (ESPICE)	The organization applies practices to identify, select and bid for acquirer requests for information, quotations and proposals based on decisions that appropriately consider customer needs, risks, organizational abilities and competitor capabilities.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.4.2 Exploitability

Key Risk	Risk Factors	Responses	Applicable Enterprise SPICE processes	Application Practices
Opportunities are not exploited	Necessary investments are not taken	Investment needs and potentials are considered systematically	Investment Management (ESPICE)	The organization applies practices to ensure that organization realize optimal value from strategically aligned business investments at an affordable cost with a known and acceptable level of risk.
	Management inefficiently use resources	Systematic project management practices applied	Project Management (ESPICE)	The management applies practices to ensure the business projects achieve their objectives within given resource constraints by initiating, planning, executing, monitoring, controlling and closing the project activities and resources.
	Product or service quality is not ensured	Systematic quality management practices applied	Quality Assurance and Management (ESPICE)	The organization applies practices to assure the quality of the product or service and of the processes used, and provide management with appropriate visibility into all relevant quality aspects.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.4.3 Satisfaction

Key Risk	Risk Factors	Responses	Applicable Enterprise SPICE processes	Application Practices
Losses due to customer dissatisfaction	Requirements are not established adequately	Requirements are established based on customer needs	Requirements (ESPICE)	The organization applies practices to develop a detailed and precise set of requirements that meet customer needs and expectations and manage those requirements throughout the life cycle.
	Ineffective business relationship management	Business relationship management is maintained	Business Relationship Management (ESPICE)	The organization applies practices to establish and maintain a mutually satisfying relationship between the product or service supplier and the business partner based on understanding the business partner and its business drivers.
	Product or service delivery default	Monitoring based on agreed service levels	Operation and Support (ESPICE)	The organization applies practices to operate the product or service at agreed service levels and support its users.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3. Governance Processes for Trusted Businesses

3.1 Governance of Controlled Business Operation Application Category

The Governance of Controlled Business Operation application category has the focus on how effectively enterprise governance applies the Internal Control (COSO 2006) Principles together with the Security, Availability, Processing Integrity, Confidentiality and Privacy Principles.

Eight processes relate to the Governance of Controlled Business Operation application category:

- *Control Risks* – The organization and its staff adequately address risks to the governance objectives relevant for financial reporting and trusted business operation and consider those risks in management of business operation.

- *Control Management* – The management of the organization is able to control business processes in a way which is adequate to the objectives of internal control over financial reporting and trusted business operation.

- *Control Competence* – Sufficient skills and knowledge relevant for the objectives of internal control over financial reporting and trusted business operation are available and used.

- *Information Reliability* – Data architecture and disclosure elements relevant for financial reporting objectives and trusted business operation, and for supporting data processing integrity are accurate and consistent.

- *Process Control* – Design and operation of process-level controls relevant to the objectives of financial reporting and trusted business operation, and processing integrity principle are effective.

- *Data Protection* – The organization and its staff are committed to security, confidentiality and privacy principles to avoid unauthorized access to and misuse of confidential data effected by business operation.

- *Integrity Assurance* – The organization and its staff are committed to comply with ethical and business integrity requirements relevant to the objectives of financial reporting and trusted business operation, and availability principle.

- *Control Efficiency* – Efficient usage of control resources relevant to the objectives of financial reporting and trusted business operation.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1.1 Control Risks

Process ID	GOV.CR
Process Name	Control Risks
Process Purpose	The purpose of the Control Risks process is to ensure that the organization and its staff adequately address risks to the governance objectives relevant for financial reporting and trusted business operation and consider those risks in management of business operation. NOTE1: The Control Risks process is a special application of the COSO 2006 model in the context of the "Risk Awareness" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 based reference model without recreating processes that are already well established. NOTE2: The descriptions of the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference model and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard.
Process Outcomes	As a result of successful implementation of the Control Risks process: 1) Governance objectives relevant for financial reporting and trusted business operation are established. 2) Risk assessments are performed consistently. 3) Organization's internal controls are integrated with risks to achievement of organization's objectives relevant for financial reporting and trusted business operation.
Application practices	**BP1 Establish governance objectives for financial reporting and trusted business operation.** Management specifies governance objectives relevant for financial reporting and trusted business operation with sufficient clarity and criteria to enable the identification of risks to the achievement of the governance objectives relevant for financial reporting and trusted business operation. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the COSO 2006 Financial Reporting Objectives process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **IFC.RA.FRO.BP1 Identify Management assertions.** To identify relevant management assertions, management starts with the governance reports, including disclosures, and identifies significant governance objectives, based on management's estimate of materiality. For each governance report and disclosure management then identifies relevant assertions, underlying transactions and events, and processes supporting these governance objectives. **IFC.RA.FRO.BP2 Consider the Range of Assessment Activities.** Management, with oversight board review, considers the range of the organization's activities to assess whether all are appropriately captured in the governance reports, and considers whether the governance reports appropriately communicate to readers economic

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

reality in a useful form.

IFC.RA.FRO.BP3 Compare Governance Policies. Management compares the governance principles adopted for the organization to those used by companies of similar size and industry. Management also compares the content and level of detail in the organization's governance reports to those organizations' reports. Significant variations are considered by management and summarized for board review.

BP2 Perform consistent risk assessment. The organization identifies and analyses risks to the achievement of governance objectives relevant for the organization's financial reporting and trusted business operation as a basis for determining how the risks should be managed. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the COSO 2006 Financial Reporting Risks process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.RA.FRR.BP1 Apply Risk Identification Process. Management's risk identification process includes identifying:

- Relevant management assertions for each significant governance objectives.
- Business processes and business units supporting governance objectives and disclosures.
- Information technology (IT) systems supporting key business processes relevant to governance objectives.

IFC.RA.FRR.BP2 Map Controls. Management maps its controls to the five internal control components, with headers that list the activity's control objectives and risks. This approach targets activities that might generate governance errors.

IFC.RA.FRR.BP3 Interact with External Parties. As part of an organisation's risk identification, management interacts with external parties that may affect the reliability of governance reporting, including suppliers, investors, creditors, shareholders, employees, customers, intermediaries, and industry peers.

IFC.RA.FRR.BP4 Consider External Factors. Management considers external factors that impact its ability to achieve its governance objectives, such as economic, competitive, and industry conditions; regulatory and political environment; and changes in technology, supply sources, customer demands, or creditor requirements. Management also considers how internal factors and changes in them impact the organisation's ability to achieve its governance objectives. These include governance report characteristics, business process characteristics, and entity-wide factors.

IFC.RA.FRR.BP5 Update Risk Assessments. Management updates risk assessments periodically (e.g. on a quarterly basis), considering:

- Newly identified risks determined to be significant.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- Escalation of previously identified risks to higher relevance.
- The status of action plans to mitigate significant risks.

This risk assessment evaluates risk based on potential impact and likelihood of risks. The resulting assessment is used as a key input in determining required control activities.

IFC.RA.FRR.BP6 Meet with Relevant Personnel. Key governance personnel meet on a regular basis with:

- Executive management to identify new initiatives, commitments, and activities affecting risks to financial reporting and trusted business operation.
- Information technology personnel to monitor changes in information technology that may affect risks related to financial reporting and trusted business operation.
- Human resources staff to identify and assess how changes in the workforce may affect competencies needed for internal control over financial reporting and trusted business operation.
- Legal counsel to stay abreast of legal/regulatory changes.

BP3 Address risks relevant for financial reporting and trusted business operation. Actions are taken to address risks to the achievement of the governance objectives relevant for financial reporting and trusted business operation. [Outcome: 3]

NOTE3: This practice is implemented by performing practices of the COSO 2006 Integration with Risk Assessment process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.CA.IRA.BP1 Consider Entity-Wide Controls. Management considers entity-wide controls that are pervasive across the organisation when considering whether control activities are sufficient to address identified risks.

IFC.CA.IRA.BP2 Use Workshops to Identify and Evaluate Controls. Management uses workshops to identify appropriate control activities for each identified risk to a governance objective and to train its employees in proper implementation of control activities.

IFC.CA.IRA.BP3 Use Matrices to Identify and Evaluate Controls. Management uses risk/control matrices developed in the process of assessing risks and designing controls in each business process to perform a “gap analysis” to evaluate the need for any additional controls that might be needed to mitigate risks to the achievement of governance objectives.

IFC.CA.IRA.BP4 Use an Inventory of Controls to Identify and Evaluate Controls. Management uses register or software that provides an inventory of controls typically aligned to specified risks to financial reporting and trusted business operation.

IFC.CA.IRA.BP5 Use independent assessment of outsourcing service provider’s internal control over processing transactions

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	for user organization. When outsourcing all or a portion of its function related to financial reporting and trusted business operation, the CFO or CGO obtains an independent assessment report (like SOC 1 Type II) or undertakes procedures to assess controls in place for the initiation, recording, and processing of significant classes of transactions at the third-party outsourcer.
Relationship Notes	The relationships between the Control Risks process and application practices, and other processes in COSO 2006 model, have been noted for each practice above. This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**COSO 2006:** IFC.RA.FRO Financial Reporting Objectives, IFC.RA.FRR Financial Reporting Risks, IFC.CA.IRA Integration with Risk Assessment
References	**Internal Control over Financial Reporting — Guidance for Smaller Public Companies** Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved.

Work Products	
Inputs	Outputs
Governance Policies and Procedures [Outcomes: 1, 2]	Governance Objectives [Outcome: 1]
Governance Objectives [Outcome: 1]	Related Business Activities [Outcome: 1]
Governance Reports [Outcome: 1, 2]	Review Records [Outcome: 1]
Management assertions [Outcome: 2]	Governance Objectives [Outcome: 1]
Organizational Structure [Outcome: 2]	Management assertions [Outcome: 1]
Related Business Activities [Outcome: 2]	Risk and Control Documentation [Outcomes: 2, 3]
Related IT Systems [Outcome: 2]	Risk Assessment Reports [Outcome: 2]
Governance Competencies [Outcome: 2]	Inventory of Controls [Outcome: 3]
Skill Assessment Reports [Outcome: 2]	
Risk and Control Documentation [Outcomes: 2,3]	
Outsourcing Assessment Report [Outcome: 3]	

Note: Above performance indicators driven by the COSO 2006 model are applicable for assessing the effectiveness of controls in relation to objectives of financial reporting and trusted business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1.2 Control Management

Process ID	GOV.CM
Process Name	Control Management
Process Purpose	The purpose of the Control Management process is to ensure that the management of the organization is able to control business processes in a way which is adequate to the objectives of internal control over financial reporting and trusted business operation. NOTE1: The Control Management process is a special application of the COSO 2006 model in the context of the "Accountability" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 based reference model without recreating processes that are already well established. NOTE2: The descriptions of the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference model and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard.
Process Outcomes	As a result of successful implementation of the Control Management process: 1) Policies and procedures relevant for the governance objectives of financial reporting and trusted business operation are consistently implemented and communicated. 2) Management structure is adequate to internal control over financial reporting and trusted business operation. 3) Management takes stimulating behavior for supporting internal control over financial reporting and trusted business operation.
Application practices	**BP1 Establish governance policies and procedures relevant for the governance objectives of financial reporting and trusted business operation.** Governance policies related to reliable financial reporting and trusted business operation are established and communicated throughout the organisation, with corresponding procedures resulting in management directives being carried out. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the COSO 2006 Policies and Procedures process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **IFC.CA.PP.BP1 Develop and Document Policies and Procedures.** Management develops and documents policies and procedures for all significant financial reporting and trusted business operation related activities using various formats such as narratives, flowcharts, and control matrices. **IFC.CA.PP.BP2 Consider Preventative and Detective Controls.** Management includes both preventative and detective controls within each process, using process maps, narratives, spreadsheets, or other mechanisms to document and communicate the control

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

activities.

IFC.CA.PP.BP3 Develop Policies for Entity-Wide Application. Central management develops policies for areas that have entity-wide application, such as its code of conduct, delegation of authority, safeguarding of assets, and so forth. In addition, management develops policies at the business unit level that support and align with entity-wide policies.

BP2 Assign governance roles and responsibilities. Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting and trusted business operation. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the COSO 2006 Authority and Responsibility process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.CE.AR.BP1 Define Objectives and Responsibilities. Management sets forth clear business and management objectives and position descriptions to reinforce management's responsibility for effective internal control over financial reporting and trusted business operation.

IFC.CE.AR.BP2 Review Key Positions. For key financial reporting and trusted business operation positions, the oversight board reviews management's descriptions of the positions' responsibilities and authorities, and considers how those positions affect the strength of internal control over financial reporting and trusted business operation, calling for re-evaluation where needed.

IFC.CE.AR.BP3 Assign Authorities and Responsibilities. In assigning authorities and responsibilities, management considers the impact on the effectiveness of the control environment and importance of maintaining effective segregation of duties. Management establishes an appropriate balance between the authority needed to "get the job done" and the need to maintain adequate internal control over key processes.

IFC.CE.AR.BP4 Empower Employees. Management empowers employees to correct problems or implement improvements in their assigned business processes as necessary, balanced with appropriate monitoring of performance.

IFC.CE.AR.BP5 Align Positions with Responsibilities and Authorities. Management considers the nature of employee positions within the organization when assigning responsibilities to individuals or determining certain levels of authority for positions.

BP3 Management takes stimulating behaviour. Management's philosophy and operating style support achieving effective internal control over financial reporting and trusted business operation. [Outcome: 3]

NOTE3: This practice is implemented by performing practices of the COSO 2006 Management's Philosophy and Operating Style process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	IFC.CE.MPO.BP1 Emphasize Risk Mitigation. Management emphasizes the importance of minimizing risks related to financial reporting and trusted business operation in its interactions with others involved in the financial reporting and trusted business operation process, and through its dealings with customers, suppliers or distributors, and employees. **IFC.CE.MPO.BP2 Emphasize Processing Requirements.** The organisation's operating philosophy requires that all journal entries, including those reflecting assumptions and estimates, be properly authorized, supported by adequate documentation and subject to review by an appropriate senior financial executive. **IFC.CE.MPO.BP3 Emphasize Importance of Diligence.** Management provides sufficient direction such that employees recognize the importance of applying appropriate diligence and business judgment in the performance of assigned job responsibilities. **IFC.CE.MPO.BP4 Establish and Articulate Governance Objectives.** Management establishes and articulates governance objectives, including those relating to complete, accurate and fair financial reporting and trusted business operation, with personnel involved in the financial reporting and trusted business operation process.
Relationship Notes	The relationships between the Control Management process and application practices, and other processes in COSO 2006 model, have been noted for each practice above. This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**COSO 2006:** IFC.CA.PP Policies and Procedures, IFC.CE.AR Authority and Responsibility, IFC.CE.MPO Management's Philosophy and Operating Style
References	**Internal Control over Financial Reporting — Guidance for Smaller Public Companies** Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved.

Work Products	
Inputs	Outputs
Inventory of Controls [Outcome: 1]	Governance Policies and Procedures [Outcome: 1]
Related Business Activities [Outcomes: 1, 3]	Review Records [Outcomes: 1, 2]
Organizational Structure [Outcomes: 1, 2]	Roles and Responsibilities [Outcome: 2]
Roles and Responsibilities [Outcomes: 1]	Nomination Records [Outcome: 2]
Job Descriptions [Outcome: 2]	Governance Objectives [Outcome: 3]
Code of Conduct [Outcome: 3]	Management Records [Outcome: 3]
Governance Objectives [Outcome: 3]	

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Note: Above performance indicators driven by the COSO 2006 model are applicable for assessing the effectiveness of controls in relation to objectives of financial reporting and trusted business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1.3 Control Competence

Process ID	GOV. CC
Process Name	Control Competence
Process Purpose	The purpose of the Control Competence process is to ensure the availability and usage of sufficient skills and knowledge relevant for the objectives of internal control over financial reporting and trusted business operation. NOTE1: The Control Competence process is a special application of the COSO 2006 model in the context of the "Competency" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 based reference model without recreating processes that are already well established. NOTE2: The descriptions of the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference model and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard.
Process Outcomes	As a result of successful implementation of the Control Competence process: 1) Recruitment, compensation and training activities are performed systematically. 2) Staff members are continually informed, feedbacks are periodically reviewed. 3) Competent individuals are retained in relation to the business operation, financial reporting and related oversight roles.
Application practices	**BP1 Use human resource policies and practices relevant for financial reporting and trusted business operation objectives.** Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting and trusted business operation. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the COSO 2006 Human Resources process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **IFC.CE.HR.BP1 Develop and Maintain Position Descriptions.** Management develops and maintains position descriptions that reflect its values and the competencies needed to execute position requirements. **IFC.CE.HR.BP2 Develop and Maintain Human Resource Policies and Procedures.** The human resource function develops and periodically updates materials outlining the organisation's human resource policies and procedures. **IFC.CE.HR.BP3 Review Resumes and Perform Reference Checks.** Management reviews resumes and performs reference checks in considering candidates for key financial reporting and trusted business operation positions. For positions with high level responsibility and authority, the organisation also performs

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

background checks.

IFC.CE.HR.BP4 Provide Training and Awareness. The human resource function provides training and awareness programs to promote ethical behaviour throughout the organization. Additional training programs related to financial reporting and trusted business operation are provided to all employees with direct and indirect involvement in financial reporting and trusted business operation.

IFC.CE.HR.BP5 Establish a Review and Appraisal Process. Management establishes a review and appraisal process that confirms knowledge of each employee's progress and status within the organization.

IFC.CE.HR.BP6 Perform Exit Interviews. An organization's process for performing exit interviews includes inquiries about any concerns related to the organization's governance and internal control.

IFC.CE.HR.BP7 Design Compensation Plans. Compensation plans for senior executives include a significant element tied to achievement of non-financial goals (for example, customer satisfaction, employee retention, and successful systems implementation) and is not excessively tied to short-term results as reflected in governance reports.

IFC.CE.HR.BP8 Review Compensation Plans. The oversight board reviews management compensation plans, including bonus and stock compensation components, to determine whether the plans create inappropriately high risk of financial reporting and trusted business operation misstatements and implements controls as needed to reduce risk to an acceptable level.

IFC.CE.HR.BP9 Evaluate Competency of Personnel. Management evaluates the sufficiency and competency of personnel involved in recording and reporting financial information.

BP2 Provide effective internal communication over control requirements relevant for financial reporting and trusted business operation objectives. Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the COSO 2006 Internal Communication process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.IC.IC.BP1 Communicate Information Regarding Governance Objectives. Management communicates information about the organisation's governance objectives, relevant internal control policies and procedures and how they work, and related individual responsibilities.

IFC.IC.IC.BP2 Communicate Through an Intranet Site. Management develops and maintains an intranet site, accessible to all appropriate personnel, for disseminating information regarding the organisation's internal control processes over financial reporting and trusted business operation.

IFC.IC.IC.BP3 Review Financial Information with the Oversight

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Board. At regular oversight board meetings, the CFO reviews financial information, analysis and related internal control, and enters into open discussion on all matters of directors' interest.

IFC.IC.IC.BP4 Communicate Between the Board and Internal Auditor. The oversight board and the chief internal auditors meet periodically and whenever events or circumstances warrant.

IFC.IC.IC.BP5 Communicate the Whistle-blower Program to Staff. The organisation maintains a "whistle-blower" process that enables employees to communicate misconduct, including matters relating to reliable governance.

IFC.IC.IC.BP6 Communicate Alternative Reporting Channels. Management provides an alternative to reporting to a line manager – either a coaching or mentoring program or a professional or technical reporting channel – so that employees are confident that they will be heard.

IFC.IC.IC.BP7 Develop Guidelines for Communication to the Oversight Board. The oversight board develops guidelines for materials it expects to receive.

IFC.IC.IC.BP8 Consult with Outside Advisors. The oversight board consults with outside advisors whenever committee members feel management might lack the capability to adequately address an important issue.

BP3 Retain competent individuals. The organization retains individuals competent in relation to the organization's business operation, financial reporting and related oversight roles. [Outcome: 3]

NOTE3: This practice is implemented by performing practices of the COSO 2006 Financial Reporting Competences process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.CE.FRC.BP1 Establish Required Knowledge, Skills and Abilities. Before hiring for key financial positions, management establishes and agrees on the knowledge, skills, and abilities (and related credentials) needed to effectively carry out the associated responsibilities.

IFC.CE.FRC.BP2 Supplement Competencies. The organization supplements in-house financial reporting and trusted business operation competencies as needed by establishing arrangements with outside specialists.

IFC.CE.FRC.BP3 Provide Training. Management provides training for employees involved in financial reporting and trusted business operation processes, either in-house or through outside service providers.

IFC.CE.FRC.BP4 Evaluate Competencies in Key Governance Roles. The oversight board (board of directors and/or audit committee) evaluates the competencies of individuals serving in key governance roles, such as CEO, CGO or CFO.

IFC.CE.FRC.BP5 Review and Evaluate Competencies.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	Management periodically reviews and evaluates employees relative to their assigned roles to determine whether the employees' skills are appropriate for their current job responsibilities.
Relationship Notes	The relationships between the Control Competence process and application practices, and other processes in COSO 2006 model, have been noted for each practice above. This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**COSO 2006:** IFC.CE.HR Human Resources, IFC.IC.IC Internal Communication, IFC.CE.FRC Financial Reporting Competencies
References	**Internal Control over Financial Reporting — Guidance for Smaller Public Companies** Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved.

Work Products	
Inputs	Outputs
Code of Conduct [Outcome: 1]	Job Descriptions [Outcome: 1]
Job Descriptions [Outcome: 1]	HR Policies and Procedures [Outcome: 1]
Roles and Responsibilities [Outcome: 1]	HR Records [Outcome: 1]
Nomination Records [Outcome: 1]	Training Plans [Outcomes: 1, 3]
Training Plans [Outcomes: 1, 3]	Periodic Staff Information [Outcome: 1]
Periodic Staff Information [Outcomes: 1, 2]	Review and Appraisal Process [Outcome: 1]
Governance Competencies [Outcome: 1]	Compensation Plans [Outcome: 1]
Skill Assessment Reports [Outcomes: 1, 3]	Review Records [Outcomes: 1, 2]
Governance Information Repository [Outcome: 2]	Skill Assessment Reports [Outcomes: 1, 3]
Financial Control Information Repository [Outcome: 2]	Guidelines for Communication to the Oversight Board [Outcome: 2]
Oversight Agenda [Outcome: 2]	Governance Competencies [Outcome: 3]
Audit Files [Outcome: 2]	Outsourcing Arrangements [Outcome: 3]
Operating and Compliance Information [Outcome: 2]	

Note: Above performance indicators driven by the COSO 2006 model are applicable for assessing the effectiveness of controls in relation to objectives of financial reporting and trusted business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1.4 Information Reliability

Process ID	GOV.IR
Process Name	Information Reliability
Process Purpose	The purpose of the Information Reliability process is to ensure the accuracy and consistency in data architecture and disclosure elements relevant for financial reporting objectives and trusted business operation, and for supporting data processing integrity. NOTE1: The Information Reliability process is a special application of the COSO 2006 and COBIT 4.1 models in the context of the "Accuracy" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles and the COBIT 4.1 framework in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 and COBIT 4.1 based reference models without recreating processes that are already well established. NOTE2: The descriptions of the COBIT 4.1 processes and the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference models and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard.
Process Outcomes	As a result of successful implementation of the Information Reliability process: 1) Effective information architecture and data model are maintained. 2) Information is systematically collected and assessed to detect compliance issues, privacy problems and fraud. 3) Control information for automated process settings, data manipulations and calculations are maintained systematically.
Application practices	**BP1 Ensure the integrity and consistency of all data stored in electronic form.** Satisfy the business requirement of being agile in responding to requirements; provide reliable, consistent information, and seamlessly integrate applications into business processes. [Outcome: 1] NOTE1: This practice is implemented by performing practices (control objectives) of the COBIT 4.1 Define the Information Architecture process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **PO2.1 Create and maintain enterprise information model.** Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure. **PO2.2 Create and maintain enterprise data dictionary (ies).** Maintain an enterprise data dictionary that incorporates the organisation's data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

users, and prevent incompatible data elements from being created.

PO2.3 Establish and maintain data classification scheme. Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption.

PO2.4 Manage data integrity. Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.

BP2 Manage processing information. Pertinent information is identified, captured, used at all levels of the organisation, and distributed in a form and timeframe that supports the achievement of the organization's financial reporting and trusted business operation objectives. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the COSO 2006 Financial Reporting Information process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.IC.FRI.BP1 Use Matrices to Detail Information Flows. Process owners maintain matrices that, for each process impacting financial reporting and trusted business operation, detail the flow of information from the point of capture through reporting.

IFC.IC.FRI.BP2 Obtain Information from External Sources. Management obtains information from external sources, such as industry publications, trade associations and conferences to identify events affecting industry trends, suppliers, customers, competitors, and the economic climate.

IFC.IC.FRI.BP3 Meet with Personnel from Other Business Area. Management in charge of governance meets periodically with personnel from other areas of the business – such as operations, compliance, human resources, or product development – to obtain information that may affect financial reporting and trusted business operation.

BP3 Manage control information. Information used to execute other control components is identified, captured, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities. [Outcome: 3]

NOTE3: This practice is implemented by performing practices of the COSO 2006 Internal Control Information process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.IC.ICI.BP1 Develop and Maintain Internal Control Information Maps. Process owners develop and maintain information maps.

IFC.IC.ICI.BP2 Identify Internal Control Information through

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

Work Products	
Inputs	Outputs
Strategic IT plan [Outcome: 1]	Data classification scheme [Outcome: 1]
Tactical IT plan [Outcome: 1]	Optimised business systems plan [Outcome: 1]
Business requirements feasibility study [Outcome: 1]	Data dictionary [Outcome: 1]
Post-implementation review [Outcome: 1]	Information architecture [Outcome: 1]
Performance and capacity information [Outcome: 1]	Assigned data classifications [Outcome: 1]
Performance input to IT planning [Outcome: 1]	Classification procedures and tools [Outcome: 1]
Related Business Activities [Outcome: 2]	Governance Information Maps [Outcomes: 2, 3]
Related IT Systems [Outcome: 2]	Meeting Minutes [Outcome: 2]
Organizational Structure [Outcome: 2]	Governance Information Repository [Outcomes: 2, 3]
Operating and Compliance Information [Outcomes: 2, 3]	Reporting Triggers [Outcome: 3]
Management Records [Outcome: 2]	Review Records [Outcome: 3]
Governance Information Maps [Outcome: 3]	

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Note: Above performance indicators driven by the COBIT 4.1 and COSO 2006 models are applicable for assessing the effectiveness of controls in relation to objectives of financial reporting and trusted business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1.5 Process Control

Process ID	GOV.PC
Process Name	Process Control
Process Purpose	The purpose of the Process Control process is to ensure effective design and operation of process-level controls relevant to the objectives of financial reporting and trusted business operation, and processing integrity principle. NOTE1: The Process Control process is a special application of the COSO 2006 model in the context of the "Process Integrity" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 based reference model without recreating processes that are already well established. NOTE2: The descriptions of the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference models and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard. NOTE3: Processing integrity principle is referred by AICPA's guide of Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2). This reference material is not directly applicable to define ISO/IEC 15504 conformant process reference model and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard, however provide detailed criteria for implementing these principles.
Process Outcomes	As a result of successful implementation of the Process Control process: 1) Control activities over access, amendments, adjustments and other usage of business information are maintained systematically. 2) Application and general IT controls are maintained. 3) Process performance metrics are collected and evaluated.
Application practices	**BP1 Maintain control activities.** Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting and trusted business operation objectives. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the COSO 2006 Selection and Development of Control Activities process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **IFC.CA.SD.BP1 Separate Incompatible Activities.** Management separates incompatible activities by assigning them to different personnel or through implementation of information technology applications. **IFC.CA.SD.BP2 Monitor When Restricting Access Is not Practical.** Where limiting access to transaction records is not practical, management, process owners, or internal auditors monitor the records closely for potential misstatements. **IFC.CA.SD.BP3 Provide Outsourcing Assessment Report.**

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Management is outsourcing some of its operations to a third party, which is contractually obligated to report to the organisation on relevant controls, and provides an independent assessment report (e.g. SOC 1 Report).

IFC.CA.SD.BP4 Assess the Cost vs Benefit of Various Control Approaches. Management assesses the costs of addressing identified risks using various control approaches, and weighs the costs against effectiveness of the controls in mitigating the respective risks.

IFC.CA.SD.BP5 Use Organizational Charts to Identify Incompatible Functions. Using organization charts, process flowcharts or other means by which activities are documented, management identifies any incompatibilities in functions and maintains appropriate segregation of duties.

IFC.CA.SD.BP6 Consider Compensating Controls. Where resource constraints compromise the ability to segregate duties to achieve governance objectives effectively, management considers compensating control activities.

BP2 Maintain information technology controls. Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting and trusted business operation objectives. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the COSO 2006 Information Technology process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.CA.IT.BP1 Apply Systems Development Controls. These controls over design and implementation of systems help to ensure that systems are appropriately developed, configured, approved, and migrated into production.

IFC.CA.IT.BP2 Apply Change Management Controls. These controls over modifications to systems – whether applications, supporting databases or operating systems – help to ensure that changes are approved and properly tested and implemented.

IFC.CA.IT.BP3 Apply Security and Access Controls. These controls over critical applications, supporting databases, and networks help management to ensure that access is properly authorized and data is appropriately used, maintained and reported.

IFC.CA.IT.BP4 Apply Computer Operations Controls. Management applies these controls over day-to-day operations to ensure that processing errors or improprieties are identified and corrected in a timely manner.

IFC.CA.IT.BP5 Apply Application Controls. Management implements controls over data input to determine whether transactions are authorized, and transactions are processed correctly and completely, with rejected items captured and followed-up

IFC.CA.IT.BP6 Identify and Secure End-User Computing Applications. Management identifies significant end-user applications, including spreadsheets and other user-developed

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	programs. **IFC.CA.IT.BP7 Review Outsourced Operations.** Management reviews general computer controls of critical third party vendors that host and/or support critical financial applications and/or information technology support functions. **BP3 Evaluate effectiveness of internal controls.** Ongoing and/or separate evaluations enable management to determine whether internal control over financial reporting and trusted business operation is present and functioning. [Outcome: 3] NOTE3: This practice is implemented by performing practices of the COSO 2006 Ongoing and Separate Evaluations process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **IFC.MO.OSE.BP1 Use Metrics to Track performance.** Management establishes supervisory activities, consisting of recording metrics about control in processes so that current performance can be tracked and compared with target performance. **IFC.MO.OSE.BP2 Develop and Implement Control Charts.** Management develops and implements control charts for reviewers – usually supervisors of those with first-level accountability for processes and activities and their controls – to use in considering whether control performance is on track, the right metrics are being monitored, and deviations are being investigated and resolved. **IFC.MO.OSE.BP3 Relate Metrics to Governance Objectives.** Management confirms that operations metrics that are monitored have reasonable correlation to financial reports and thus can be used as an indicator of potential deficiencies in financial reporting and trusted business operation. **IFC.MO.OSE.BP4 Use Self-Assessments.** Management develops a self-assessment questionnaire for a business process for use by personnel involved in executing controls. **IFC.MO.OSE.BP5 Use Computer Network Testing.** Management periodically tests its computer network by performing a penetration review to identify weaknesses in internal controls regarding external connectivity. **IFC.MO.OSE.BP6 Use Internal Audit.** Management uses an internal audit function to provide an objective perspective on key elements of the internal control system. **IFC.MO.OSE.BP7 Determine Scope and Frequency of Separate Evaluations.** Management sets a schedule for conducting separate evaluations of specific processes and control activities, with higher risk processes reviewed by the internal audit function.
Relationship Notes	The relationships between the Process Control process and application practices, and other processes in COSO 2006 model, have been noted for each practice above. This innovative concept of including “Application Areas” in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**COSO 2006:** IFC.CA.SD Selection and Development of Control Activities,

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	IFC.CA.IT Information Technology, IFC.MO.OSE Ongoing and Separate Evaluations
References	**Internal Control over Financial Reporting — Guidance for Smaller Public Companies** Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved. **Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)** Copyright © 2011, American Institute of Certified Public Accountants, Inc. All Rights Reserved.

Work Products	
Inputs	Outputs
Inventory of Controls [Outcome: 1]	Risk and Control Documentation [Outcome: 1]
Organizational Charts [Outcome: 1]	Cost vs. Benefit Analysis [Outcome: 1]
Risk and Control Documentation [Outcomes: 1, 2, 3]	Review Records [Outcomes: 1, 2, 3]
Outsourcing Arrangements [Outcome: 1]	Outsourcing Assessment Report [Outcome: 1]
Related IT Systems [Outcome: 2]	IT Controls Documentation [Outcome: 2]
Outsourcing Assessment Report [Outcomes: 2, 3]	Operational Metrics [Outcome: 3]
Operating and Compliance Information [Outcome: 3]	Assessment Control Charts [Outcome: 3]
Audit Files [Outcome: 3]	Self-Assessment Files [Outcome: 3]
	Computer Network Test Files [Outcome: 3]
	Assessment Plan [Outcome: 3]

Note: Above performance indicators driven by the COSO 2006 model are applicable for assessing the effectiveness of controls in relation to objectives of financial reporting and trusted business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1.6 Data Protection

Process ID	GOV.DP
Process Name	Data Protection
Process Purpose	The purpose of the Data Protection process is to ensure that the organization and its staff are committed to security, confidentiality and privacy principles to avoid unauthorized access to and misuse of confidential data effected by business operation. NOTE1: The Data Protection process is a special application of the COSO 2006 and COBIT 4.1 models in the context of the "Data Protection" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles and the COBIT 4.1 framework in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 and COBIT 4.1 based reference models without recreating processes that are already well established. NOTE2: The descriptions of the COBIT 4.1 processes and the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference models and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard. NOTE3: Security, confidentiality and privacy principles are referred by AICPA's guide of Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2). This reference material is not directly applicable to define ISO/IEC 15504 conformant process reference model and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard, however provide detailed criteria for implementing these principles.
Process Outcomes	As a result of successful implementation of the Data Protection process: 1) Preventive controls are maintained to avoid system security incidents. 2) Anti-fraud management program is maintained. 3) Privacy requirements are kept.
Application practices	**BP1 Maintain policies and procedures to avoid system security incidents.** Satisfy the business requirement of maintaining the confidentiality, integrity and availability of information and the processing infrastructure aligned to business needs and minimising the impact of security vulnerabilities. [Outcome: 1] NOTE1: This practice is implemented according to the security and confidentiality principles and related criteria referred by AICPA's guide of Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2). NOTE2: This practice is implemented by performing practices (control objectives) of the COBIT 4.1 Ensure Systems Security process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **DS5.1 Management of IT Security**. Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

DS5.2 IT Security Plan. Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

DS5.3 Identity Management. Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

DS5.4 User Account Management. Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

DS5.5 Security Testing, Surveillance and Monitoring. Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

DS5.6 Security Incident Definition. Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process.

DS5.7 Protection of Security Technology. Make security- related technology resistant to tampering, and do not disclose security documentation unnecessarily.

DS5.8 Cryptographic Key Management. Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

DS5.9 Malicious Software Prevention, Detection and Correction.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

DS5.10 Network Security. Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorise access and control information flows from and to networks.

DS5.11 Exchange of Sensitive Data. Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.

BP2 Manage fraud risks. The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting and trusted business operation objectives. [Outcome: 2]

NOTE3: This practice is implemented by performing practices of the COSO 2006 Fraud Risks process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.RA.FR.BP1 Review Incentives and Pressures Related to Compensation Programs. The oversight board and management review the organization's compensation programs and organization's performance evaluation process to identify potential incentives and pressures for employees to commit fraud.

IFC.RA.FR.BP2 Conduct Fraud Risk Assessments. Management conducts a comprehensive fraud risk assessment to identify the various ways that fraud and misconduct can occur.

IFC.RA.FR.BP3 Consider Approaches to Circumvent or Override Controls. In identifying, evaluating, and testing the design and operating effectiveness of entity-wide controls that address fraud, management considers how individuals might seek to circumvent or override controls intended to prevent or detect fraud.

IFC.RA.FR.BP4 Use Information Technology Tools. Management uses, where practical, information technology tools including security systems, fraud detection and monitoring tools, and incident tracking systems to identify and manage fraud risk.

IFC.RA.FR.BP5 Develop Incident Investigation and Remediation Processes. Management develops a structured process for incident investigation and remediation. Investigation roles and responsibilities are clearly delineated, and the processes include a tracking mechanism that allows management to report on material fraud events.

IFC.RA.FR.BP6 Consider Fraud Risk by Internal Audit. The person responsible for the internal audit function incorporates results of the fraud risk assessment into the internal audit plan. Management reviews and confirms that the internal audit plan addresses relevant risks.

BP3 Maintain policies and procedures to ensure privacy requirements.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP). [Outcome: 3] NOTE4: This practice is implemented according to the privacy principle and related criteria referred by AICPA's guide of Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2). NOTE5: The generally accepted privacy principles (GAPP) are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices. The following are the 10 GAPP: **GAPP01. Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures. **GAPP02. Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed. **GAPP03. Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information. **GAPP04. Collection.** The entity collects personal information only for the purposes identified in the notice. **GAPP05. Use and retention.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfil the stated purposes. **GAPP06. Access.** The entity provides individuals with access to their personal information for review and update. **GAPP07. Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual. **GAPP08. Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical). **GAPP09. Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice. **GAPP10. Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.
Relationship Notes	The relationships between the Data Protection process and application practices, and other processes in COSO 2006 and COBIT 4.1 models, have been noted for each practice above. This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**COBIT 4.1:** DS5 Ensure Systems Security **COSO 2006:** IFC.RA.FR Fraud Risks

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	Generally Accepted Privacy Principles
References	**Control Objectives for Information and related Technology - COBIT® 4.1** Copyright © 2007 by the IT Governance Institute. 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA. All rights reserved. **Internal Control over Financial Reporting — Guidance for Smaller Public Companies** Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved. **Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)** Copyright © 2011, American Institute of Certified Public Accountants, Inc. All Rights Reserved.

Work Products	
Inputs	Outputs
Information architecture; assigned data classifications [Outcomes: 1, 2, 3]	Security incident definition [Outcome: 1]
Technology standards [Outcome: 1]	Specific training requirements on security awareness [Outcome: 1]
Risk assessment [Outcome: 1, 2, 3]	Process performance reports [Outcome: 1]
Application security controls specification [Outcome: 1]	Required security changes [Outcome: 1]
OLAs [Outcome: 1]	Security threats and vulnerabilities [Outcome: 1]
Compensation Plans [Outcome: 2]	IT security plan and policies [Outcome: 1]
Business Policies [Outcome: 2]	Fraud Risk Assessment Report [Outcome: 2]
Transaction data [Outcome: 2, 3]	Anti-Fraud Policies and Procedures [Outcome: 2]
Audit Files [Outcome: 2, 3]	Anti-Fraud Management Plan [Outcome: 2]
Identified Personal Information [Outcome: 3]	Review Records [Outcome: 2, 3]
Applicable Privacy Laws [Outcome: 3]	Privacy policies [Outcome: 3]
	Privacy procedures and controls [Outcome: 3]
	Privacy Incident Reports [Outcome: 3]

Note: Above performance indicators driven by the COBIT 4.1 and COSO 2006 models and the generally accepted privacy principles are applicable for assessing the effectiveness of controls in relation to objectives of financial reporting and trusted business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1.7 Integrity Assurance

Process ID	GOV.IA
Process Name	Integrity Assurance
Process Purpose	The purpose of the Integrity Assurance process is to ensure that the organization and its staff are committed to comply with ethical and service integrity requirements relevant to the objectives of financial reporting and trusted business operation, and availability principle. NOTE1: The Integrity Assurance process is a special application of the COSO 2006 and COBIT 4.1 models in the context of the "Commitment" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles and the COBIT 4.1 framework in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 and COBIT 4.1 based reference models without recreating processes that are already well established. NOTE2: The descriptions of the COBIT 4.1 processes and the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference models and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard. NOTE3: Availability principle is referred by AICPA's guide of Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2). This reference material is not directly applicable to define ISO/IEC 15504 conformant process reference model and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard, however provide detailed criteria for implementing these principles.
Process Outcomes	As a result of successful implementation of the Integrity Assurance process: 1) Ethical values are articulated and kept. 2) Active policies and procedures are in place to ensure business continuity. 3) Information from external parties are collected and reviewed systematically.
Application practices	**BP1 Ensure commitment to sound 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 and trusted business operation. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the COSO 2006 Integrity and Ethical Values process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **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. **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.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

IFC.CE.IEV.BP3 Demonstrate Commitment to Integrity and Ethics. Management demonstrates its commitment to sound integrity and ethical values by following a prescribed investigation process and taking appropriate, timely corrective action when possible violations are identified.

BP2 Ensure business continuity. Satisfy the business requirement of ensuring minimal business impact in the event of an IT service interruption. [Outcome: 2]

NOTE2: This practice is implemented according to the availability principle and related criteria referred by AICPA's guide of Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2).

NOTE3: This practice is implemented by performing practices (control objectives) of the COBIT 4.1 Ensure Continuous Service process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

DS4.1 IT Continuity Framework. Develop a framework for IT continuity to support enterprise-wide business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.

DS4.2 IT Continuity Plans. Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

DS4.3 Critical IT Resources. Focus attention on items specified as most critical in the IT continuity plan to build in resilience and establish priorities in recovery situations. Avoid the distraction of recovering less-critical items and ensure response and recovery in line with prioritised business needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements. Consider resilience, response and recovery requirements for different tiers, e.g., one to four hours, four to 24 hours, more than 24 hours and critical business operational periods.

DS4.4 Maintenance of the IT Continuity Plan. Encourage IT management to define and execute change control procedures to

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner.

DS4.5 Testing of the IT Continuity Plan. Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.

DS4.6 IT Continuity Plan Training. Provide all concerned parties with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the results of the contingency tests.

DS4.7 Distribution of the IT Continuity Plan. Determine that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.

DS4.8 IT Services Recovery and Resumption. Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.

DS4.9 Offsite Backup Storage. Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.

DS4.10 Post-resumption Review. Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly.

BP3 Utilize external opinions. Matters affecting the achievement of the financial reporting and trusted business operation objectives are communicated with outside parties. [Outcome: 3]

NOTE4: This practice is implemented by performing practices of the COSO 2006 External Communication process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	IFC.IC.EC.BP1 Communicate the Whistle-blower Program to Outside Parties. Management enables receipt of important information from parties doing business with the organisation, such as vendors who feel they have not been treated fairly, receive pressure for kickbacks, are subject to other improprieties, or are aware of improper financial reporting and trusted business operation. **IFC.IC.EC.BP2 Survey Outside Parties.** Management surveys customers, vendors and others on their perception of the integrity and ethical values. **IFC.IC.EC.BP3 Review External Audit Communications.** Following the external auditor's review of management's certification process and independent evaluation of internal control effectiveness, management receives a memorandum on significant matters identified during the course of the work.
Relationship Notes	The relationships between the Integrity Assurance process and application practices, and other processes in COSO 2006 and COBIT 4.1 models, have been noted for each practice above. This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**COBIT 4.1:** PO2 Ensure Continuous Service **COSO 2006:** IFC.CE.IEV Integrity and Ethical Values, IFC.IC.EC External Communication
References	**Control Objectives for Information and related Technology - COBIT® 4.1** Copyright © 2007 by the IT Governance Institute. 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA. All rights reserved. **Internal Control over Financial Reporting — Guidance for Smaller Public Companies** Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved. **Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)** Copyright © 2011, American Institute of Certified Public Accountants, Inc. All Rights Reserved.

Work Products	
Inputs	Outputs
Remediation Plans [Outcome: 1]	Code of Conduct [Outcome: 1]
Periodic Staff Information [Outcome: 1]	Monitoring Reports [Outcome:1]
Assigned data classifications [Outcome: 2]	Remediation Plans [Outcome: 1]
Risk assessment Availability, continuity and recovery specification [Outcome: 2]	Periodic Staff Information [Outcome: 1]

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

User, operational, support, technical and administration manuals [Outcome: 2]	Contingency test results [Outcome: 2]
SLAs and OLAs [Outcome: 2]	Criticality of IT configuration items [Outcome: 2]
Operating and Compliance Information [Outcome: 3]	Backup storage and protection plan [Outcome: 2]
Oversight Agenda [Outcome: 3]	Incident/disaster thresholds [Outcome: 2]
Audit Files [Outcome: 3]	Disaster service requirements, including roles and responsibilities [Outcome: 2]
	Process performance reports [Outcome: 2]
	Outside Parties Survey [Outcome: 3]
	Review Records [Outcome: 3]

Note: Above performance indicators driven by the COBIT 4.1 and COSO 2006 models are applicable for assessing the effectiveness of controls in relation to objectives of financial reporting and trusted business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.1.8 Control Efficiency

Process ID	GOV.CE
Process Name	Control Efficiency
Process Purpose	The purpose of the Control Efficiency process is to ensure efficient usage of control resources relevant to the objectives of financial reporting and trusted business operation. NOTE1: The Control Efficiency process is a special application of the COSO 2006 model in the context of the "Control Efficiency" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 based reference model without recreating processes that are already well established. NOTE2: The descriptions of the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference models and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard.
Process Outcomes	As a result of successful implementation of the Control Efficiency process: 1) Adequate organizational structure and reporting lines are maintained. 2) Oversight of internal controls is effective. 3) Control deficiencies are reviewed and necessary actions are taken.
Application practices	**BP1 Ensure adequate organizational structure.** The entity's organizational structure supports effective internal control over financial reporting and trusted business operation. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the COSO 2006 Organizational Structure process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **IFC.CE.OS.BP1 Develop Organizational Charts.** Management develops an organizational chart, which sets forth roles and respective reporting lines for all employees, including those involved in financial reporting and trusted business operation. **IFC.CE.OS.BP2 Align Roles to Processes.** Each unit or function within the organization aligns roles to key processes supporting governance objectives. **IFC.CE.OS.BP3 Maintain Job Descriptions.** Management maintains job descriptions for key positions and updates them as conditions and circumstances warrant. **IFC.CE.OS.BP4 Establish Organizational Structures.** Management adopts a structure whereby there are adequate staff layers between the Chief Governance Officer (CGO) and personnel directly involved in the financial reporting and trusted business operation process. **IFC.CE.OS.BP5 Establish Structure for Internal Audit.** An internal audit function reports directly to the Chief Executive Officer (CEO),

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

with direct access to the oversight board (e.g. audit committee), to maintain independence over financial reporting and trusted business operation.

BP2 Supervise internal controls. The oversight board understands and exercises oversight responsibility related to trusted business operation, financial reporting and related internal control. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the COSO 2006 Oversight Board process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation:

IFC.CE.OB.BP1 Establish Content for Board Meetings. The oversight board establishes a formal policy for specific decisions or events that require discussion with or approval from the board, as well as a calendar for the timing of these discussions.

IFC.CE.OB.BP2 Identify Independent Board Members. Independent oversight board and/or audit committee members are identified.

IFC.CE.OB.BP3 Establish Boards Roles and Responsibilities. The oversight board through the corporate bylaws, and the audit committee through its charter, set forth their roles and responsibilities.

IFC.CE.OB.BP4 Consider Effectiveness of Internal Control. The oversight board regularly considers the effectiveness of internal control over financial reporting and trusted business operation, including risks, significant deficiencies, and material weaknesses (if any).

IFC.CE.OB.BP5 Meet with Auditors. The oversight board meets regularly with the internal and external auditors, including in private meetings. The board reviews audit scope and testing plans, resources and staffing, and significant audit findings.

IFC.CE.OB.BP6 Review Policies and Procedures. The oversight board reviews governance policies and procedures used by management for determining significant expectations, including key assumptions.

IFC.CE.OB.BP7 Maintain Scepticism. The oversight board maintains an appropriate level of scepticism regarding management's assertions and judgments affecting governance reporting, asking probing and challenging questions of management.

IFC.CE.OB.BP8 Consider Whistle-blower Information. The oversight board considers information obtained from the whistle-blower program and the organisation's anti-fraud and similar processes to monitor the risks of misstatements in governance reporting, including risks of inappropriate acts by staff and management override of controls. The board reviews reports of significant matters, considering the potential impact on governance reporting and need for corrective action.

IFC.CE.OB.BP9 Review Board Candidates. The oversight board conducts due diligence on board and audit committee candidates to confirm appropriate independence from the organisation and

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	management and his/her ability to be an effective board member. **IFC.CE.OB.BP10 Certify Compliance.** The oversight board members certify annually their compliance with the organisation's ethics guidelines and independence rules. **IFC.CE.OB.BP11 Meet with Management.** The oversight board allocate a portion of every meeting for discussions of issues without management present, including separate time with external advisors, internal audit, the external auditor and outside legal counsel. **BP3 Manage internal control deficiencies.** Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to the management and the oversight board as appropriate. [Outcome: 3] NOTE3: This practice is implemented by performing practices of the COSO 2006 Reporting Deficiencies process with a specific focus on how enterprise governance supports internal control over financial reporting and trusted business operation: **IFC.MO.RD.BP1 Report Information from Alternative Channels.** Management establishes an alternative channel for reporting deficiencies sensitive in nature, such as illegal or improper acts. **IFC.MO.RD.BP2 Report Deficiencies to Various Levels in the Organisation.** Management establishes a practice where all financial reporting and trusted business operation deficiencies regardless of materiality are reported to the responsible manager and at least one level of management above, both of whom are positioned to take corrective action. **IFC.MO.RD.BP3 Develop Guidelines for Reporting Deficiencies.** Management develops a list of control deficiencies that seriously threaten the reliability of governance reporting, which if they occur are required to be reported to senior management and the board.
Relationship Notes	The relationships between the Control Efficiency process and application practices, and other processes in COSO 2006 model, have been noted for each practice above. This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**COSO 2006:** IFC.CE.OS Organizational Structure, IFC.CE.OB Oversight Board, IFC.MO.RD Reporting Deficiencies
References	**Internal Control over Financial Reporting — Guidance for Smaller Public Companies** Copyright © 2006 by The Committee of Sponsoring Organization, C/O AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311 – 3881, USA. All rights reserved.

Work Products	
Inputs	Outputs
Whistle-blower Information [Outcome: 2]	Organizational Structure [Outcome: 1]
Governance Policies and Procedures [Outcome: 2]	Organizational Charts [Outcome: 1]

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Management Reports [Outcome: 2]	Job Descriptions [Outcomes: 1]
Audit Files [Outcome: 2]	Audit Charter [Outcome: 2]
Periodic Staff Information [Outcome: 3]	Oversight Agenda [Outcome: 2]
Audit Files [Outcome: 3]	Board Members File [Outcome: 2]
Remediation Plans [Outcome: 3]	Meeting Minutes [Outcome: 2]
	Review Records [Outcome: 2]
	Periodic Oversight Report [Outcome: 2]
	Internal Control Deficiencies Records [Outcome: 3]
	Governance Deficiencies and Resolutions Reports [Outcome: 3]
	Remediation Plans [Outcome: 3]

Note: Above performance indicators driven by the COSO 2006 model are applicable for assessing the effectiveness of controls in relation to objectives of financial reporting and trusted business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.2 Governance of Sustainable Business Operation Application Category

The Governance of Sustainable Business Operation application category has the focus on keeping business operation economically effective.

Three processes relate to the Governance of Sustainable Business Operation application category:

- *Competitive Operation* – Ensuring market recognition of the business operation.
- *Exploitable Operation* – Organization realizes optimal value from business operation.
- *Satisfactory Operation* – Ensuring user/customer satisfaction based on agreed levels of business operation.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.2.1 Competitive Operation

Process ID	GOV. COP
Process Name	Competitive Operation
Process Purpose	The purpose of the Competitive Operation process is to ensure market recognition of the business operation. NOTE: The Competitive Operation process is a special application of the Enterprise SPICE model in the context of the "Competitiveness" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the Enterprise SPICE model in the context of this special application. This facilitates the re-use of the model without recreating processes that are already well established.
Process Outcomes	As a result of successful implementation of the Competitive Operation process: 1) Business goals and targets are systematically maintained. 2) Customers and other stakeholder needs and expectations are considered for improvement of product or service features. 3) Effective proposal preparation practices are maintained.
Application practices	**BP1 Establish and maintain business goals and targets.** The organization applies practices to establish strategic enterprise direction and ensure the enterprise achieves its goals and objectives. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the Enterprise SPICE Enterprise Governance process with a specific focus on business sustainability: **GVM.1.BP1: Establish and Maintain Strategic Vision.** Establish, maintain, and communicate a strategic vision that identifies long-term goals, values, performance expectations, and core activities. **GVM.1.BP2: Establish and Maintain Policies.** Establish, maintain and communicate policies and directives. **GVM.1.BP3: Align to Achieve the Vision.** Align the enterprise to operate efficiently and consistently to achieve the vision. Establish leadership systems and structures for decision making, empowerment, and conflict resolution. Provide incentives for contributing to enterprise vision and strategy. **GVM.1.BP4: Ensure sharing of common vision.** Ensure that individuals in the enterprise share a common culture, understand the common vision, and are committed and empowered to perform their functions effectively. **GVM.1.BP5: Establish and Maintain Strategy.** Establish and maintain the enterprise strategic plans that identify business objectives to be achieved, areas of business to be pursued and their interrelationships, and the significant goals to be accomplished. **GVM.1.BP6: Formulate and align enterprise budgets.** Formulate enterprise budgets to ensure alignment with strategic goals. Ensure congruency with action plans.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

GVM.1.BP7: Develop and Deploy Action Plans. Establish, integrate, and deploy tactical action plans to accomplish strategic objectives.

GVM.1.BP8: Review Performance. Review performance relative to goals and changing needs across the enterprise.

GVM.1.BP9: Act on Results of Review. Translate performance review findings into action.

GVM.1.BP10: Fulfill Public Responsibility. Address the impacts on society of planned activities, products, services, and operations, considering regulatory and legal requirements and risks associated with products, services, and operations.

GVM.1.BP11: Inform employees regarding enterprise performance. Inform employees regarding enterprise performance.

BP2 Evolve customer and other stakeholder needs and expectations. The organization applies practices to elicit, analyze, clarify, and document evolving customer and other stakeholder needs and expectations. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the Enterprise SPICE Needs process with a specific focus on business sustainability:

LFC.1.BP1: Identify customers and stakeholders: Identify customers and stakeholders.

LFC.1.BP2: Elicit needs: Elicit customer and other stakeholders' needs, expectations, and measures of effectiveness.

LFC.1.BP3: Analyze needs: Analyze needs and expectations in the context of the intended operational environment.

LFC.1.BP4: Establish and maintain a statement of need: Establish and maintain a statement of customer and other stakeholder needs and expectations that is understood and agreed upon by the customer and other stakeholders.

LFC.1.BP5: Communicate with customers: Communicate and interact with customers and other stakeholders throughout the life cycle to assure a common understanding of the status and disposition of needs, expectations, and measures of effectiveness.

LFC.1.BP6: Determine customer satisfaction: Determine customer satisfaction with products and services.

BP3 Keep proposal preparation practices effective. The organization applies practices to identify, select and bid for acquirer requests for information, quotations and proposals based on decisions that appropriately consider customer needs, risks, organizational abilities and competitor capabilities. [Outcome: 3]

NOTE3: This practice is implemented by performing practices of the Enterprise SPICE Tendering process with a specific focus on business sustainability:

GVM.7.BP1: Evaluate Organizational Skills, Services and Products. Examine and document the organizational goals, service

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	catalog, resumes and existing products to determine what target markets to pursue or develop. **GVM.7.BP2: Establish Criteria and Risk Analysis for Submission.** Document the basis for determining a bid or no bid decision for responding to requests for proposals. **GVM.7.BP3: Evaluate Acquirer Requests for Proposals and Inquiries.** Determine that proposed effort is in accordance with potential targets identified in organizational goals. Determine if the requested task is in line with existing organizational skills and talents or if these skills will have to be acquired. Review overall requirements to determine if they are consistent, concise and clearly defined. Document any questions that need to be posed to the acquirer for clarification. Determine the probability that the organization can be successful in this bid according to established criteria. Identify the logical contenders for the proposal and their advantages. **GVM.7.BP4: Perform any Preliminary Research and Development, Surveys or Trade Studies.** Determine if the request requires investigation of key product or service components that may prove to be high risk when providing the requested product or service. Investigate trade studies or surveys covering the expected work involved. **GVM.7.BP5: Make a Go/No Go Decision.** Based on established criteria and risk analysis, including preliminary research, decide whether to pursue or not pursue a request for a proposal. **GVM.7.BP6: Identify Resources to Perform Proposed Work and Form Proposal Team.** Identify needed skills and form a qualified team to develop the proposal, and to perform the proposed work. **GVM.7.BP7: Establish and Maintain Supplier/acquirer Communications Interface.** Assign an individual or organizational entity to establish a communications interface with the potential acquirers. Review the acquirer's schedule of events and point of contact to assure adherence to proposal preparation and delivery schedule. **GVM.7.BP8: Perform Estimation.** Estimate costs and resources needed to satisfy the request. **GVM.7.BP9: Prepare and Submit Proposal in Response to Acquirer Request.** Prepare proposal in accordance with guidelines in the acquirer's request document or request. **GVM.7.BP10: Negotiate and Confirm Agreement.** Negotiate relevant aspects of the agreement and formally confirm the agreement.
Relationship Notes	The relationships between the Competitive Operation process and application practices, and other processes in Enterprise SPICE model, have been noted for each practice above. This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**Enterprise SPICE:** GVM.1 Enterprise Governance, LFC.1 Needs, GVM.7 Tendering

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

References	**Enterprise SPICE® - An Integrated Model for Enterprise-wide Assessment and Improvement** Technical Report – Issue 1 September 2010 Copyright © The SPICE User Group 2010.

Note1: Above base practices referred by the Enterprise SPICE model are applicable for assessing governance effectiveness related to the sustainability objectives of the business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Note2: The Enterprise SPICE model does not contain the capability dimension of the Process Assessment Model beyond capability level 1. As not targeting higher process capability levels during this special application, this material does not include the list of specific work products as referred by the process performance indicators of the Enterprise SPICE processes. Therefore the judgment of governance effectiveness related to the sustainability objectives of the business operation is based on assessment of organization' governance practices by considering the listed base practices.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.2.2 Exploitable Operation

Process ID	GOV.EOP
Process Name	Exploitable Operation
Process Purpose	The purpose of the Exploitable Operation process is to ensure that organization realizes optimal value from business operation. NOTE: The Exploitable Operation process is a special application of the Enterprise SPICE model in the context of the "Exploitability" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the Enterprise SPICE model in the context of this special application. This facilitates the re-use of the model without recreating processes that are already well established.
Process Outcomes	As a result of successful implementation of the Exploitable Operation process: 1) Investments for business operation needs and business potentials are performed deliberately. 2) Project management practices are applied for business operation. 3) Quality management practices are applied for business operation.
Application practices	**BP1 Manage investments supporting business goals and targets.** The organization applies practices to ensure that organization realize optimal value from strategically aligned business investments at an affordable cost with a known and acceptable level of risk. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the Enterprise SPICE Investment Management process with a specific focus on business sustainability: **GVM.2.BP1: Establish Criteria.** Establish and maintain criteria for selecting and evaluating potential investments. **GVM.2.BP2: Identify Investment Proposals.** Collect business cases, identifying and describing investment proposals. **GVM.2.BP3: Categorize Proposals.** Define investment categories, categorization criteria, and categorize proposals. **GVM.2.BP4: Prioritize and Evaluate Investment Proposals.** Evaluate and prioritize investment proposals. **GVM.2.BP5: Establish and Maintain the Investment Portfolio.** Select proposals to be included in the investment portfolio. Establish and maintain the investment portfolio. **GVM.2.BP6: Identify and Allocate Resources.** Allocate resources to execute selected investments. Reallocate resources from deactivated and terminated investments. **GVM.2.BP7: Review/evaluate Performance.** Review and evaluate ongoing investments versus stated criteria to determine whether to continue with, add to, or terminate specific investments. **GVM.2.BP8: Adjust Investment Portfolio.** Adjust the investment portfolio in response to actual portfolio performance.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

GVM.2.BP9: Communicate Portfolio Adjustment. Communicate results of portfolio adjustment to relevant stakeholders.

GVM.2.BP10: Monitor Changes. Monitor changes in strategy, risk levels, and resource constraints to assure appropriate alignment.

BP2 Manage business project activities and resources. The management apply practices to ensure the business projects achieve their objectives within given resource constraints by initiating, planning, executing, monitoring, controlling and closing the project activities and resources. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the Enterprise SPICE Project Management process with a specific focus on business sustainability:

GVM.8.BP1: Define Project Objectives, Scope, and Outputs. Define project objectives, scope, and the work products and services that are to be provided by the project.

GVM.8.BP2: Define the Life-Cycle Approach and Activities. Define the life-cycle approach that will be used and define and sequence the activities needed to achieve project outputs.

GVM.8.BP3: Define Stakeholders. Identify stakeholders and interfaces between project elements and with other project and organizational units.

GVM.8.BP4: Estimate Planning Parameters. Estimate and document the work product and task planning parameters that provide a basis for resource estimates.

GVM.8.BP5: Estimate Project Resource Requirements. Estimate the project effort, cost, schedule and other resource requirements.

GVM.8.BP6: Establish Schedules. Develop schedules for the project.

GVM.8.BP7: Establish Budget. Develop a budget for the project.

GVM.8.BP8: Plan the Quality. Identify the quality requirements and/or standards for the project or product and document how the project will demonstrate compliance.

GVM.8.BP9: Develop the Human Resource Plan. Identify the experience, knowledge and skill requirements for the project and apply them to the selection of individuals and teams. Identify the specific individuals and groups contributing to, and impacted by, the project, allocate their specific responsibilities, and ensure that commitments are understood, accepted, funded and achievable.

GVM.8.BP10: Plan Communications. Determine project stakeholder information needs and define a communication approach.

GVM.8.BP11: Plan Risks. Identify and analyze risks which may affect the project. Develop alternatives and actions in order to enhance opportunities and to reduce threats to the project objectives.

GVM.8.BP12: Plan Procurements. Plan and document project purchasing decisions.

GVM.8.BP13: Establish and Maintain Plans. Establish and

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

maintain a complete set of plans for providing the products and services throughout the project life cycle.

GVM.8.BP14: Establish Commitment. Establish and maintain commitment of affected groups and individuals to project objectives and plans and commitment of resources as identified in the plan.

GVM.8.BP15: Acquire, Develop and Manage Project Team. Identify individuals or teams that will be assigned the resources and responsibilities for meeting project objectives. Improve the competencies of the team. Track team member performance, provide feedback, resolve issues and manage changes to optimize project performance.

GVM.8.BP16: Direct and Manage Project Execution. Perform the work defined in the project plan to achieve the project's objectives.

GVM.8.BP17: Distribute Information. Make relevant or established information available to project stakeholders as planned.

GVM.8.BP18: Manage Stakeholder Expectations. Communicate and work with stakeholders to meet their needs and address issues as they occur.

GVM.8.BP19: Monitor Project Performance. Monitor and track project activities and results against plans and baseline.

GVM.8.BP20: Review and Analyze Project Performance. Conduct formal and informal reviews of project performance and analyze variances from the plans.

GVM.8.BP21: Take Corrective Action. Take corrective actions to address problems.

GVM.8.BP22: Close Project. Close the project formally using appropriate organizational mechanisms and update organizational process assets.

BP3 Provide quality management and assurance for business operation. The organization applies practices to assure the quality of the product or service and of the processes used, and provide management with appropriate visibility into all relevant quality aspects. [Outcome: 3]

NOTE3: This practice is implemented by performing practices of the Enterprise SPICE Quality Assurance and Management process with a specific focus on business sustainability:

SUP.3.BP1: Establish a Quality Management System. Establish, document, implement, and maintain a quality management system.

SUP.3.BP2: Monitor Process Compliance. Objectively monitor compliance of performed activities with the established processes.

SUP.3.BP3: Monitor Product and Service Quality. Objectively compare, measure and evaluate work products and services against the requirements and standards that define them.

SUP.3.BP4: Monitor Noncompliance Issues. Monitor and track noncompliance issues and support their resolution via escalation to senior management if necessary.

SUP.3.BP5: Record and Report Results. Record and report the

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	results of quality assurance activities and customer satisfaction data to applicable stakeholders. **SUP.3.BP6: Analyze Quality.** Analyze quality records and measurements to detect the need for corrective action and develop recommendations for quality improvement or corrective and preventive actions. **SUP.3.BP7: Initiate Quality Improvement.** Initiate activities that address identified quality issues or quality improvement opportunities. **SUP.3.BP8: Monitor and Evaluate the Effect of Changes.** Monitor the status of quality improvements on products and services and evaluate the effect of changes after they have been implemented.
Relationship Notes	The relationships between the Exploitable Operation process and application practices, and other processes in Enterprise SPICE model, have been noted for each practice above. This innovative concept of including "Application Areas" in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**Enterprise SPICE:** GVM.2 Investment Management, GVM.8 Project Management, SUP.3 Quality Assurance and Management
References	**Enterprise SPICE® - An Integrated Model for Enterprise-wide Assessment and Improvement** Technical Report – Issue 1 September 2010 Copyright © The SPICE User Group 2010.

Note1: Above base practices referred by the Enterprise SPICE model are applicable for assessing governance effectiveness related to the sustainability objectives of the business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Note2: The Enterprise SPICE model does not contain the capability dimension of the Process Assessment Model beyond capability level 1. As not targeting higher process capability levels during this special application, this material does not include the list of specific work products as referred by the process performance indicators of the Enterprise SPICE processes. Therefore the judgment of governance effectiveness related to the sustainability objectives of the business operation is based on assessment of organization' governance practices by considering the listed base practices.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.2.3 Satisfactory Operation

Process ID	GOV.SOP
Process Name	Satisfactory Operation
Process Purpose	The purpose of the Satisfactory Operation process is to ensure user/customer satisfaction based on agreed levels of business operation. NOTE: The Satisfactory Operation process is a special application of the Enterprise SPICE model in the context of the "Satisfaction" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the Enterprise SPICE model in the context of this special application. This facilitates the re-use of the model without recreating processes that are already well established.
Process Outcomes	As a result of successful implementation of the Satisfactory Operation process: 1) Requirements are established and maintained based on user/customer needs and expectations. 2) Business relationship management is effective. 3) Business operation supports its user entities by achievement of agreed service level requirements.
Application practices	**BP1 Establish and maintain requirements that meet customer needs and expectations.** The organization applies practices to develop a detailed and precise set of requirements that meet user/customer needs and expectations and manage those requirements throughout the life cycle. [Outcome: 1] NOTE1: This practice is implemented by performing practices of the Enterprise SPICE Requirements process with a specific focus on business sustainability: **LFC.2.BP1: Identify Requirements.** Identify all types of requirements applicable to customer needs and expectations. **LFC.2.BP2: Derive Requirements.** Derive requirements that may be identified as necessary implications of the identified requirements. **LFC.2.BP3: Analyze Requirements.** Analyze requirements to ensure that they satisfy established quality criteria, including unambiguity, completeness, traceability, feasibility, and verifiability. **LFC.2.BP4: Baseline Requirements.** Record, approve, baseline, and place under change control all requirements. **LFC.2.BP5: Analyze Requirements Risks.** Document and analyze risks associated with the requirements. **LFC.2.BP6: Manage Requirements Changes.** Analyze all requirements change requests for impact on the product or service and, upon approval, incorporate the approved changes into the requirements baseline. **LFC.2.BP7: Ensure and Maintain Requirements Traceability across the Life Cycle.** Maintain traceability among requirements and between requirements and plans, work products, and activities

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

initiating corrective action if inconsistencies are identified.

BP2 Manage relationship among business stakeholders. The organization applies practices to establish and maintain a mutually satisfying relationship between the product or service supplier and the business partner based on understanding the business partner and its business drivers. [Outcome: 2]

NOTE2: This practice is implemented by performing practices of the Enterprise SPICE Business Relationship Management process with a specific focus on business sustainability:

GVM.5.BP1: Develop Relationships. Develop and document contacts and relationships with the business, customers and stakeholders.

GVM.5BP2: Establish Interactive Communication Methodologies and Structures with Stakeholders and Partners. Name an individual or individuals who are responsible for collaboratively managing customer satisfaction and the whole Business Relationship Management process.

GVM.5BP3: Identify Relationship Attributes. Identify and manage cultural, market, loyalty and beneficiaries attributes.

GVM.5.BP4: Identify Value Creation Opportunities. Proactively identify value creation opportunities and communicate them to the customer.

GVM.5.BP5: Manage Complaints and Compliments. Log and manage all complaints and compliments by analyzing existing information, obtaining feedback from customers and performing service reviews.

GVM.5.BP6: Create Service Level Agreements. Create Service Level Agreements between the business owner and the product/service supplier.

GVM.5.BP7: Establish a Service Catalog. Establish and maintain a service catalog for communicating with the business.

BP3 Operate according to agreed service levels. The organization applies practices to operate the product or service at agreed service levels and support its users/customers. [Outcome: 3]

NOTE3: This practice is implemented by performing practices of the Enterprise SPICE Operation and Support process with a specific focus on business sustainability:

LFC.8.BP1: Operate the Product or Service. Operate the product or service in its intended environment according to agreed service levels.

LFC.8.BP2: Establish Methods. Establish methods for monitoring and sustaining required product or service levels.

LFC.8.BP3: Monitor and Evaluate Capacity, Service, and Performance. Monitor and evaluate capacity, service, and performance of the product or service.

LFC.8.BP4: Confirm Availability of Resources. Confirm availability

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

	of required resources (e.g., personnel, parts) to ensure service levels can be sustained. **LFC.8.BP5: Perform Corrective and/or Preventive Maintenance. P**erform corrective and/or preventive maintenance by replacing or servicing product or service elements prior to failure. **LFC.8.BP6: Analyze Failures.** Perform failure identification and analysis activities when problems or interruptions occur in the product or delivered service. **LFC.8.BP7: Take or Initiate Corrective Action.** Take corrective action when appropriate (e.g., defective part, human error), or initiate corrective action for product or service modification. **LFC.8.BP8: Provide Customer Support.** Answer customer and user questions and help resolve problems they encounter.
Relationship Notes	The relationships between the Satisfactory Operation process and application practices, and other processes in Enterprise SPICE model, have been noted for each practice above. This innovative concept of including “Application Areas” in a process assessment model instantiates the idea of using already established processes with respect to a particular application.
Sources	**Enterprise SPICE:** LFC.2 Requirements, GVM.5 Business Relationship Management, LFC.8 Operation and Support
References	**Enterprise SPICE® - An Integrated Model for Enterprise-wide Assessment and Improvement** Technical Report – Issue 1 September 2010 Copyright © The SPICE User Group 2010.

Note1: Above base practices referred by the Enterprise SPICE model are applicable for assessing governance effectiveness related to the sustainability objectives of the business operation. However they should be considered as a starting point for judgment whether, given the application context, they are contributing to the intended purpose of the process, not as a compulsory check-list of what every organization must have.

Note2: The Enterprise SPICE model does not contain the capability dimension of the Process Assessment Model beyond capability level 1. As not targeting higher process capability levels during this special application, this material does not include the list of specific work products as referred by the process performance indicators of the Enterprise SPICE processes. Therefore the judgment of governance effectiveness related to the sustainability objectives of the business operation is based on assessment of organization’ governance practices by considering the listed base practices.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3.3 Linking Governance Processes to Sustainable Value Creation

Governance capability issues have come into the view of the management as the huge cost of regulatory compliance activities request consideration of sustainability and added business value of such efforts. This challenge has been answered by utilizing the ISO/IEC 15504 standard based Governance Capability Assessment (Governance SPICE) concept applicable for the executive managers, the boards of directors, the audit committees, the internal and external auditors and the supervisory bodies for assessing the effectiveness of internal controls even in different business units and activities, IT management and financial reporting processes.

Major governance scandals, independently from the recent global financial and economic crisis, call the attention that not only the basic business operations (production, sales, supply chain, etc.) need to be assessed, audited or certified to the conformance with specific standards, but all the governance related processes. The cases of the most newsworthy scandals showed that even those big multinational companies, which are committed to quality and process improvement issues, can fail to avoid governance breakdowns such as fraudulent financial reporting.

In these circumstances the term of “trusted business” has got additional attention by the customers in any type of business relationship. Beyond the traditional marketing methods, the product and service providers need to distinguish themselves from their market competitors not just with higher quality or excellence level, faster market response or better pricing, but they are also enforced to present themselves as reliable and sustainable business partners. Customers respect those business partners in long term relationship, whose corporate culture is at similar or even at higher level than theirs.

Regulatory requirements like the Sarbanes-Oxley Act for US SEC registrants and their affiliates (all over the world), the Basel framework, the Company Law in the EU, the European and national directives for governmental and public sector organizations, etc. require not just the implementation of risk management and internal control systems based on internationally recognized frameworks, but also the periodic disclosure of effectiveness conclusion performed by the executive management. However some of these regulations are still limited to financial reporting, the global crisis showed that wider focus of risk management and internal controls has real business value. During the last decade many-many thousands of such periodic assessments were performed worldwide in industry, financial and governmental sectors and the regulators are keen to further develop mandatory rules and guidelines increasing stakeholder’s benefit from disclosures.

The global crisis also reminds that many former periodic assessments concluding positive opinion on effectiveness of internal controls were failed at those companies, where the insularly used economic models for risk assessment were not aligned with the time horizon of the strategic business objectives. Accountability of executive management and oversight boards should be established and supported by using integrated assessment models applicable for both operational and financial processes. Those assessment models which can cover the most activity areas relevant for strategic objectives have added value to line managers, executive management, internal and external auditors and oversight bodies, as they help to optimize monitoring efforts of different operations based on a common measurement model of achieving objectives.

Using the Governance Model has some immediate evidential benefits. At first, it provides ready to use structure for implementing selected or all elements of the recognized control frameworks and generic enterprise models. Regulatory or voluntary compliance requirements could be looked through clear business driven governance objectives helping better understanding and meaningful design and operation by enterprise management. Besides the less implementation efforts, this structure unburdens the internal and external audit activities in concluding opinion about the fulfilment of compliance requirements.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

At second, the Governance Model offers sufficient set of practices to determine the enterprise specific control objectives. The management can easily select and communicate those minimum requirements which are considered as crucial for running business on the specific market (composing the risk appetite). This decision is a clear message to all stakeholders, including potential customers, that which operational risks are planned to be mitigated by the enterprise management, and which risks remain unattended.

Furthermore, setting target governance capability levels to the governance processes or even to the applied entity-level control processes helps to interpret qualitative and quantitative measures for design and operational effectiveness conclusions. By this way, the business process management solutions, like workflow systems, project toolkits, reporting tools, etc. can be configured for automatically collecting and providing performance information both about the process-level and entity-level controls, based on the manually and/or electronically processed business activities.

Tracking of the evidences for governance process performance by a process management suite, which is also able to map these evidences to process assessment models – like in the case of the “Stages” platform – provides solution to automate formal assessment of governance capability over a period of time. These assessment results certified by a qualified issuer can be published directly by the assessed enterprise, or via a “trusted business” promotion portal.

Customers will be able to select their business partners by browsing and comparing governance capability assessment results in the fields of their interest, or use sector specific benchmarking results for preparing new calls for tenders.

The implemented and assessed business cases during the BPM GOSPEL are going to be promoted as the first best practice case studies following the above value creation process.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. Applicability for Outsourcing Service Organizations

4.1 Need for Reporting on Service Organization's Controls

Many companies function more efficiently and profitably by outsourcing tasks or entire functions to service organizations that have the personnel, expertise, equipment, or technology to accomplish these tasks or functions. Examples of such services include cloud computing, managed security, health care claims management and processing, sales force automation etc. Although user management can delegate these tasks or functions to a service organization, they are usually held responsible by those charged with governance (for example, the board of directors), customers, shareholders, regulators and other affected parties for establishing effective controls over those outsourced functions. The following SOC reports provide user management with the information they need about the service organization's controls to help assess and address the risks associated with an outsourced service:

SOC 1 Report - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

These reports, prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization [7], are specifically intended to meet the needs of the of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user' auditors), in evaluating the effect of the controls at the service organization on the user entities' financial statements. Use of these reports is restricted to the management of the service organization, user entities, and user auditors.

SOC 2 Report - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

These reports are intended to meet the needs of a broad range of users that need information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems [8]. These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

4.2 Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

The SSAE 16 standard requires management of the service organization to provide a **description of its "system"** along with a **written assertion** to the service auditor, both of which require careful attention and preparation by management themselves.

Description of the System

The framework for documenting a service organization's system for purposes of SSAE 16 (SOC 1) should include a comprehensive discussion of the following components:

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

- The services provided along with the classes of transactions processed.
- The procedures used, from beginning to end, both automated and manual, for the transactions (i.e., the flow of the transactions and all activities, from initiation to correction of errors, as necessary).
- How the system captures addresses significant events and conditions along with what processes and procedures are used to prepare and report information as necessary to user entities.
- The control objectives, related controls and user control considerations
- The service organizations elements of internal control, which are generally based on the COSO framework consisting of the following: **1. Control Environment. 2. Control Activities. 3. Information and Communication. 4. Risk Assessment. 5. Monitoring**

SSAE 16 written assertion by management

Management of the service organization must also produce a "written assertion" for purposes of SSAE 16 reporting, which is to "assert" that (1). management description of the service organization's "system" is fairly presented, (2). that the controls and related control objectives were suitably designed and (for purposes of SSAE 16 Type 2 reporting), were operating effectively.

4.3 Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

The following are the five attributes of a reliable system, which are also referred as the *trust services principles*:

- *Security.* The system is protected against unauthorized access (both physical and logical).
- *Availability.* The system is available for operation and use as committed or agreed.
- *Processing integrity.* System processing is complete, accurate, timely, and authorized.
- *Confidentiality.* Information designated as confidential is protected as committed or agreed.
- *Privacy.* Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and criteria set forth in Generally Accepted Privacy Principles issued jointly by the AICPA and the Canadian Institute of Chartered Accountants.

In a SOC 2 engagement, management of the service organization selects the trust services principle(s) that will be covered by the SOC 2 report. The trust services criteria for the principle(s) covered by the report are referred to as the *applicable trust services criteria*.

Service organization management implements controls over its systems to prevent adverse events from occurring or detect such events as errors, privacy breaches, and theft or loss of information. Management of the service organization may engage a CPA to report on the design and operating effectiveness of controls over its systems. Controls that are suitably designed are able to meet the criteria they were designed to meet if they operate effectively. Controls that operate effectively actually do meet the criteria they were designed to meet over a period of time.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4.4 Use of Governance Model by Service Management

The Governance Model consists two main application categories referring to governance objectives for "Controlled Operation" and for "Sustainable Operation". While sustainability objectives are significant for keeping service operation economically effective, the service organization's control objectives have the major focus on how effectively service governance supports user entities' internal control over financial reporting (relevant for SOC 1 reports) and applies Security, Availability, Processing Integrity, Confidentiality and Privacy Principles (relevant for SOC 2 reports).

Within the Governance of Controlled Operation application category there are 8 processes applying the practices of the 20 COSO Internal Control over Financial Reporting Principles and 3 selected COBIT processes, together also covering criteria for the Security, Availability, Processing Integrity, Confidentiality Principles and the Generally Accepted Privacy Principles.

By assuring compliance with the 8 governance processes of Controlled Operation, service management is able to provide assertions that the service controls and related control objectives relevant for user entities' are suitably designed based on the applicable criteria and operating effectively over a period of time.

Implemented with the financial support of the Commission of the European Communities under the LEONARDO DA VINCI Programme (Project number: LLP-LdV-TOI-2010-HU-001). This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.