Applying Integrated Assurance Management Scenarios for Governance Capability Assessment

János Ivanyos

Trusted Business Partners Ltd, Budapest, Hungary,
ivanyos@trusted.hu

Abstract. 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 and literatures of control frameworks and reference models are not easily interpretable by enterprise management for setting their own business' specific governance objectives. This article gives an overview of how integrated assurance management scenarios provide scoping tool for Governance Capability Assessment by applying Enterprise SPICE, COSO and COBIT reference models based governance processes.

Keywords: Assurance Management, Governance Capability, ISO/IEC 15504 (SPICE), Enterprise SPICE, COSO, COBIT, Trusted Business

1. Governance Model for Strengthening Business Trust and Sustainability

Trusted Business is highly substantial for all stakeholders, such as the owners and investors, the employees, the customers and suppliers, the creditors, and the authorities and associations of public interest for social, economic and ecologic sustainability. As the aware business risk taking is an essential element of the economic growth and innovation, it is definitely stressful how the involved parties "grease the skids" for successful management of uncertainties effecting business goals, like operational, environmental, legal, societal, human, health, etc. risks - in either micro or macro environment. The lower is the level of business trust measuring acceptance and undertaken of unavoidable uncertainties in business relationships, the higher is the cost of risk-taking due to mistrust (like in the form of higher interest rates, insurance and enforcement costs, etc.), which leads to lower efficiency and competitiveness by the unsubstantiated increase of operational costs. Therefore Transparency and Accountability requirements over enterprise governance processes might request standard measures of governance capability.

The **Governance Model for Trusted Businesses** [1] keeps both enterprise management and assurance (e.g. audit) 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 assurance providers (e.g. auditors) for compliance attestation.

The Governance Model for Trusted Businesses provides descriptions and applicable practices for the governance processes supporting management assertions and assurance reports on effective risk management and control over trusted business operation and financial reporting enabling achievement of Enterprise Goals according to stakeholders' needs and expectations. The **Governance Capability Assessment** (Governance SPICE) [2] is used to evaluate these management assertions established by Integrated Assurance Management scenarios implemented at different organizational and operational levels.

2. Governance Capability Assessment

For implementing Enterprise Governance the executive management and - if it exists - the supervisory board should follow scenarios to evaluate, direct and monitor business operation in alignment with the adapted governance objectives. In this term the "*Enterprise Governance*" is driven by the organization's specific business goals and enabling governance objectives instead of generic control or regulatory framework based "checklists". When ISO/IEC 15504 standard (SPICE) [3] based Governance Capability Assessment concept is applied, the evaluation of compliance will focus on how the capability profiles of the implemented core business and governance processes are aligned with the governance objectives customized for the Enterprise Goals. This customization keeps in mind three dimensions:

- the business operation (processes and activities) under scope,
- the applicable governance practices from recognized reference models and
- the capability level targets.

The governance processes defined by the Governance Model for Trusted Businesses are supported by selected processes from the Enterprise SPICE [4], COSO [5] and COBIT [6] reference models. These application areas associated with the process attributes defined in ISO/IEC 15504-2 provide a common basis for performing assessments of governance capability regarding Enterprise Governance and reporting of results by using a common rating scale. ISO/IEC 15504 (SPICE) offers not only transparent method for assessing performance of relevant governance processes, but also tools for assessing related risk areas based on the gaps between target and assessed capability profiles.

However traditional compliance-driven approaches have been facing to major problem as there is no evidence that compliance (to any model) really drives business success. On the contrary: all big failure companies of the last decades had been "equipped with" long list of compliance and excellence records for many years. The key problem is that managing compliance issues has only limited focus on lower level outcomes - like activity goals - without considering the overall success factors. Enterprise Governance should focus on wider internal and external contexts of risks defined as effects of uncertainties on enterprise objectives as referred by the *ISO 31000 Risk Management standard* [7].

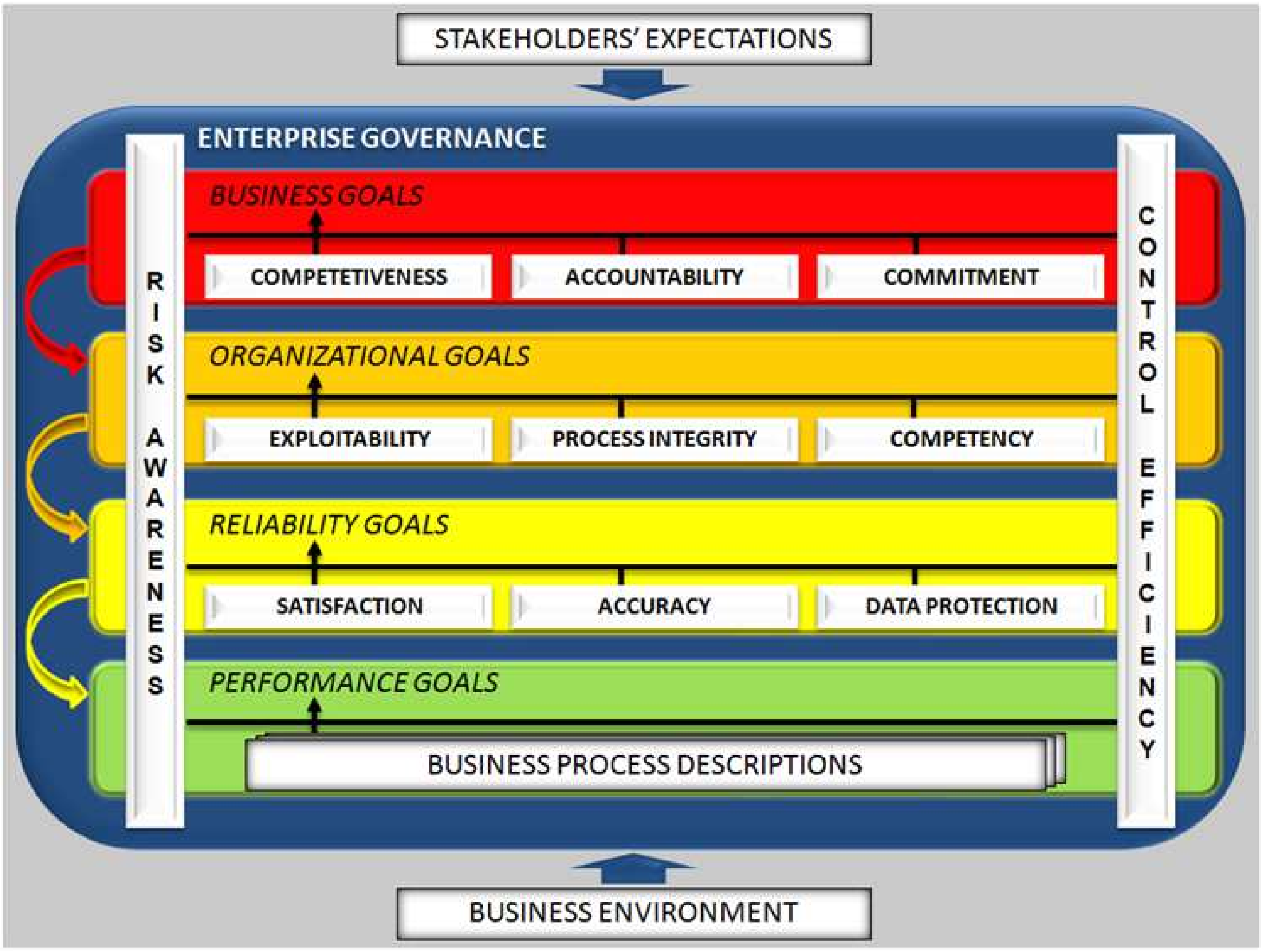

Figure 1: Linking Governance Objectives to Enterprise Goals & Measures

3. The Baseline Business Case

Memolux Ltd. is a Hungarian privately owned small business company established in 1989. It provides high quality level outsourcing services covering the full scope of business administration to more than 200 clients. Memolux has more than 20 years' experience of providing payroll services for a wide range of user entities having 1-2 to over than 1000 employees, e.g. one of the biggest clients was a telecommunication company with more than 4000 calculations per month. Memolux is the partner of ADP Employer Services International in Hungary to provide ADP Streamline® for several years. ADP Streamline® is a Global Payroll and HR administration outsourcing service designed for international organizations.

Management assertions for process-level service controls have been identified by responding control risks at activity steps of the monthly payroll calculations in the areas covered by the risk-based selected application practices offered by the Governance Model for Trusted Businesses. Day-to-day operation of monthly payroll processing cycles provides automatic logs, checklists, generated control data and reports within the work-flow management system.

Stages process modelling platform [8] was used for mapping work-flow based control evidences to generic process reference model, like the Governance Model for Trusted Businesses. For that purpose both the reference model and the **Monthly Payroll Calculation** business process have been configured. The configured processing and control requirements are useful for not only management or audit scope, but they are also applied in knowledge sharing during in-house trainings or informing new employees [9].

Compliance Workbench functions of Stages allow at first to select the relevant set of governance practices and even work products as company specific scope of the reference model. This is the result of the risk assessment performed by the management concerning to the governance objectives (based on specific business goals and business environment's expectations). At second by using Compliance Workbench functions, the elements of the business processes can be mapped to the scoped governance objectives and can be referred as management assertions for effective operation of the designed controls. At third, the evidence "pools" generated or maintained by the work-flow management system can be hyperlinked to these business process elements.

This baseline process modelling and compliance management experience pointed out some of the drawbacks of the traditional model/standard based compliance works, such as:

- too complex process documentation might be hardly usable in enterprise risk management practice
- assurance and control documentation are mostly driven by externally defined control (model based) objectives
- different perspectives of operational and organizational levels are not managed
- interconnections of performance metrics are not utilized
- too many technical layers and interfaces make fuzziness in sound judgement
- business goals and success factors are not considered by compliance assurance works

A possible solution for these challenges is provided by implementing the Integrated Assurance Management scenarios, which are applying the Enterprise SPICE, COSO and COBIT reference models based practices as adaptable enablers in context of keeping the effects of uncertainties on the Enterprise Goals at an affordable level and not as control requirement checklists.

4. Enterprise Goals driven Integrated Assurance Management scenarios

The suggested Integrated Assurance Management scenarios are mapping already existing or newly developed management practices to governance objectives - through company specific enterprise goals. By this way the compliance and assurance works will be aligned with the enterprise specific business objectives and might keep the less meaningful elements of general governance or control frameworks out of scope. However by comparing existing practices to those offered by these frameworks, the management and - if requested due to company size or corporate laws - the supervision bodies might benefit from getting wider professional knowledge and best practice suggestions for improving enterprise governance.

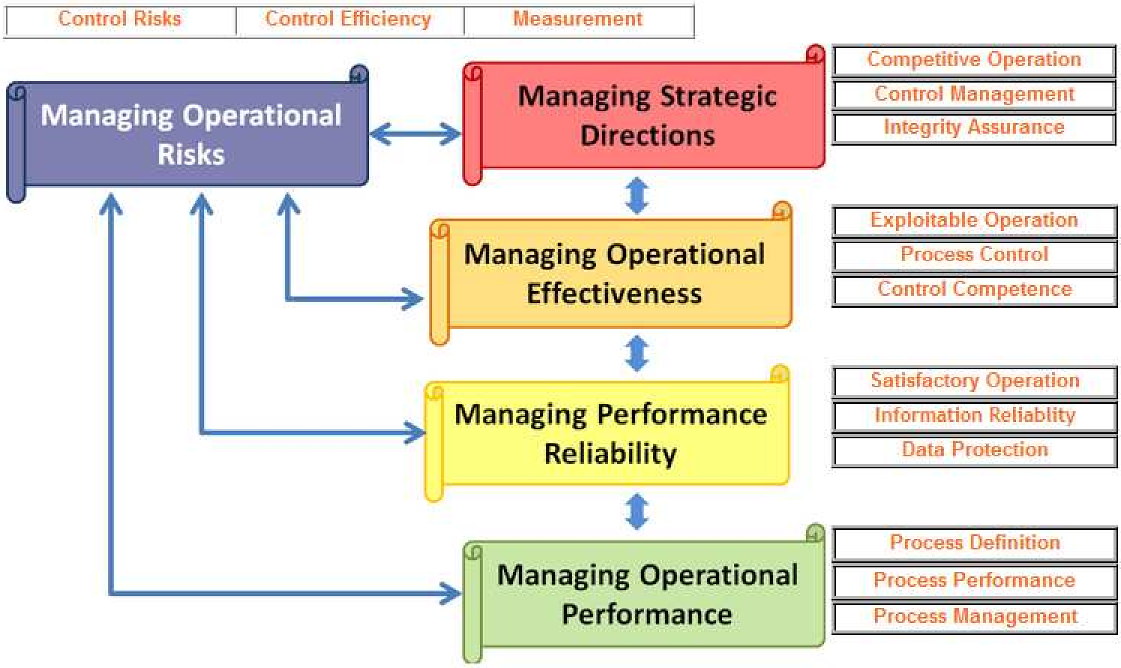

Figure 2: Enterprise Goals driven Integrated Assurance Management scenarios

The proposed Integrated Assurance Management scenarios are distinguishing different operational and organizational levels having specific targets and time-horizons. Each level defines “Usefulness” and “Efficiency” goals and measures [10] allowing management to see recognized professional framework practices as enablers instead of just compliance requirements. The following Integrated Assurance Management scenarios are referred by this case study:

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

Operational Performance is related to the core and supporting business processes of a business unit. The processes might be described by using different methodology and tools; however the process purpose and the necessary and sufficient outcomes of achieving this purpose are generally identifiable. Each specific business operation consists of a set of interrelated business processes with allocated resources, specified product or service delivery requirements and schedules. Managing Operational Performance scenario is focusing on achievement of these - relatively - short term performance objectives, for example a unique product or service delivery based on a specific client’s order. Most regulatory requirements (like health protection, safety, human rights, technical or accounting standards, etc.) might be also incorporated within activity goals and assured at this level.

Performance Reliability also refers to the above operational level with extended focus on additional aspects of performance. For repeating, parallel or extended cycles of operational processes, the operational management should establish longer term objectives such as customer retention and capacity utilization. At most cases these objectives are related to contractual or pay-off periods. For example customer satisfaction and capacity utilization rates are applicable measures for reoccurring business transactions for the monthly pay-off period of an outsourcing service.

Such as the Operational Performance instances drive the achievement of reliability objectives, the pay-off cycles based Reliable Performance drives to achieve entity (business unit) level *Operational Effectiveness* goals measured by profitability and agile resource allocation at business unit level for a quarterly or yearly reporting period. The business unit level effectiveness is also a driver to achieve objectives set by *Strategic Directions (Business Goals)*, like revenue targets and operational cash flow positions set for the strategic planning periods.

Managing Operational Risks sets risk tolerances (acceptable deviation from objectives) and risk appetites (affordable levels of uncertainties effecting objectives) for operational and organizational levels based on operational performance, reliability, effectiveness and strategic objectives. Each level's objectives have specific time-horizons, therefore the application of "traditional" consequence and probability metrics ("heat maps") for risk ratings and selecting or prioritizing the risk treatment options is reasonable only when operational or organizational levels and timescales of risk events are comparable.

Risk Management practices might show significant differences in details at SME or bigger company cases; however the same principles remain valid. Evidently a small entity or business unit also defines acceptable tolerance levels of its business targets, and establishes its governance structure adequately to affordable levels of internal and external uncertainties affecting these targets. Practically "affordable level" is different for a smaller entity with a few service or production lines than for a big multinational company with much more diversified activities.

5. Conclusions

In this business case the application of the Governance Model for Trusted Businesses was tested within a real outsourcing service environment. This sample business environment has internationally standardized SOC 1 [11] and SOC 2 [12] requirements which should be carefully considered by small business companies providing local services to multinational clients, whose compliance managers, internal and external auditors are making great demands on local service providers and raising difficulties for these companies by increasing requested control and audit efforts and costs. At most cases these demands are driven by the multinational organizations' global compliance or audit requirements, so they are not really intended to be "customized" for local conditions.

The implementation practices of Integrated Assurance Management scenarios present how even local small business organization can efficiently implement compliant governance/control frameworks with respect of its real business needs and risks, and how the implementation results can be exhibited for external evaluation or audit in a cost effective way. The baseline compliance management approach presented by Stages process modelling tool has been further developed for implementing and evaluating application practices evidencing achievement of governance objectives. By changing from the traditional *model based compliance* to *enterprise goals driven integrated assurance*, the management assertions (the links between business activities and governance practices) are implemented by applying a significantly different scoping approach.

The Integrated Assurance Management scenarios are enhancing the meaning of "compliance" to *in what extent the model based governance/control practices are relevant for supporting the achievement of enterprise goals within their acceptable tolerance levels*. The proposed Integrated Assurance Management scenarios help to select and apply model based control practices by considering the operational and organizational performance levels and their adequate time-horizons for setting enterprise objectives. The term of "*Integrated Assurance Management*" also refers to how the governance capability assessment model is adapted, understood and used by the assurance providers of all organizational and operational levels, including the oversight board, the executive and line management, the internal and external auditors, and other roles relevant in governance, risk management, control system and compliance related works.

Capability profiles of the business processes together with the enabling governance and control processes are representing "reverse", but well understandable measures of *management's risk appetite* as the higher capability levels indicate the more robust risk treatment for achieving relevant business objectives.

ISO/IEC 15504 process capability assessments (or similar audit approaches) are widely used in specific industries and sectors, like automotive, medical, space, finance, etc. Most of these assessments are performed only at operational levels aiming up to level 2 targets by using domain specific process assessment models adapting generic standards or recommendations, like ISO 12207, ITIL, COBIT, etc. The coverage of the 11 governance objectives referred by the Governance Model for Trusted Businesses helps to use the industry and sector specific process assessment models by establishing the applicable organizational contexts of level 3 and level 4 process attributes concerning to the operational and supporting business processes.

6. References

[1] Governance Model for Trusted Businesses, BPM-GOSPEL Deliverable, 2011

[2] 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.

[3] 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
ISO/IEC TR 15504-7:2008 Information technology -- Process assessment -- Part 7: Assessment of organizational maturity

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

[5] The Committee of Sponsoring Organizations of the Treadway Commission (COSO):

- Internal Control — Integrated Framework (1992)
- Enterprise Risk Management – Integrated Framework (2004)
- Internal Control over Financial Reporting — Guidance for Smaller Public Companies (2006)

[6] COBIT - Control Objectives for Information and related Technology,
COBIT 4.1 © 2007 IT Governance Institute. www.itgi.org

[7] ISO 31000:2009, Risk management – Principles and guidelines
ISO Guide 73:2009, Risk management - Vocabulary

[8] White Paper: Effectively Managing Process Compliance, Method Park and Integrated System Diagnostics, Inc., 2011

[9] Business Case Implementation Report for Effectively Managing Enterprise Governance in Compliance with Multiple Models and Best Practices, BPM-GOSPEL Deliverable, 2012

[10] C. Wells, L. Ibrahim and L. LaBruyere, New Approach to Generic Attributes, Systems Engineering, Vol. 6, No. 4, 2003. © 2003 Wiley Periodicals, Inc.

[11] 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

[12] 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.