Applying Integrated Risk Management Scenarios for Improving Enterprise Governance

János Ivanyos

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

Abstract: The term of *"scenario"* is used for systematically considering integrated risk management aspects of enterprise governance practices implemented at operational and organizational levels. These considerations are focusing on the customized design and continuous improvement of governance objectives, processes and practices enabling the better achievement of the concerning enterprise goals. Professionals having been acquiring and evidencing their Governance SPICE Assessor skills are able to provide unique consulting and assurance services for enterprises in optimizing the effects of uncertainties on governance objectives by assessing and evaluating capability of enterprise governance processes.

Keywords: Enterprise Governance, ISO/IEC 15504 (SPICE), ISO 31000 Risk Management, Enterprise Risk Management (ERM), Governance Capability Assessment

1. Risk Management Principles Improving Enterprise Governance

Enterprise Governance principles are often referred as requirements and recommendations prepared by the supervision authorities or international professional organizations only for the publicly listed, the state-owned and the big multinational companies. However following these principles - far beyond the prescribed compliance requirements - is important for all market-driven economic entities due to establishment and maintenance of trusted business relations.

"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. For these reasons, even the SMEs can benefit from presenting their governance capability conforming to international standards without exaggerated implementation and assurance costs by adapting the **Governance Model for Trusted Businesses** [1] aligned with their own business goals and environment.

For effective Risk Management integrated with Enterprise Governance, according to **ISO 31000:2009 Risk Management** standard [2], the company should at all operational and organizational levels comply with the following principles:

a) **Risk Management creates and protects value**.
Risk management contributes to the demonstrable achievement of enterprise objectives and improvement of business performance.

b) **Risk Management is an integral part of all organizational processes.**
Risk management is not separated from the main activities and business processes of the organization. Risk management is part of the responsibilities of management and an integral part of business and governance processes at all operational and organizational levels.

c) **Risk Management is part of decision making.**
Risk management assists management make informed choices, prioritize actions and distinguish among alternative courses of action.

d) **Risk Management explicitly addresses uncertainty.**
Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) **Risk Management is systematic, structured and timely.**
A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable business results.

f) **Risk Management is based on the best available information.**
The inputs to the risk management process are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

g) **Risk Management is tailored.**
Risk management is aligned with the organization's external and internal business context and risk profile.

h) **Risk Management takes human and cultural factors into account.**
Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's business objectives.

i) **Risk Management is transparent and inclusive.**
Appropriate and timely involvement of stakeholders and, in particular, decision makers at all operational and organizational levels, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

j) **Risk Management is dynamic, iterative and responsive to change.**
Risk management continually senses and responds to change. As external and internal events occur, business context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

k) **Risk Management facilitates continual improvement of the organization.**
Management should develop and implement strategies to improve the risk management capability aligned with all other (e.g. process) improvement aspects of the enterprise.

The above listed principles adopted from ISO 31000:2009 Risk Management standard comprise the base for interpreting the **Integrated Risk Management Scenarios** aiming at specific enterprise objectives within different timescales for the operational and organizational levels of business operation. Therefor risk management is integrated into the Enterprise Governance by supporting effective decision making and improvement of business performance.

ISO 31000 Risk Management principles do not directly address the term of *"risk appetite"*, however the **COSO** [3] definition and interpretation can be also applicable for these principles in context of Enterprise Governance. COSO's Enterprise Risk Management - Integrated Framework defines risk appetite as follows:

"The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. … Risk appetite guides resource allocation. … Risk appetite [assists the organization] in aligning the organization, people, and processes in [designing the] infrastructure necessary to effectively respond to and monitor risks."

"This definition raises some important points. Risk appetite:

- *is strategic and is related to the pursuit of organizational objectives;*
- *forms an integral part of corporate governance;*
- *guides the allocation of resources;*
- *guides an organization's infrastructure, supporting its activities related to recognizing, assessing, responding to, and monitoring risks in pursuit of organizational objectives;*
- *influences the organization's attitudes towards risk;*
- *is multi-dimensional, including when applied to the pursuit of value in the short term and the longer term of the strategic planning cycle; and*
- *requires effective monitoring of the risk itself and of the organization's continuing risk appetite."*

Source: Enterprise Risk Management - Understanding and Communicating Risk Appetite (COSO 2012)

In this interpretation risk appetite is definitely not just a set of acceptable (practically hardly measureable and comparable) risk levels, but much more a strategic thinking about how the uncertainties around the business objectives and their effects on these objectives should be managed at all operational and organizational levels. Implementation of enterprise governance and control processes should follow the related management decisions aligned with specific business conditions and stakeholders' expectations. Reference to formulized *Risk Appetite Statements* (at strategic level) or *Management Assertions* (at operational and organizational levels) as well documented management decisions over comprehensive enterprise risk management framework will help to change the traditional *control model based compliance* workshops to *enterprise goals driven integrated risk management.*

The **ISO/IEC 15504 standard** [4] based *process improvement* and *capability determination* methodology provides a conceptual *measurement framework* for determining organizational risk appetite by setting target capability levels for key business and governance processes. Evaluation of the gaps between target and actually assessed capability profiles provides input for the next risk treatment planning and implementation cycle at the concerning operational or organizational level.

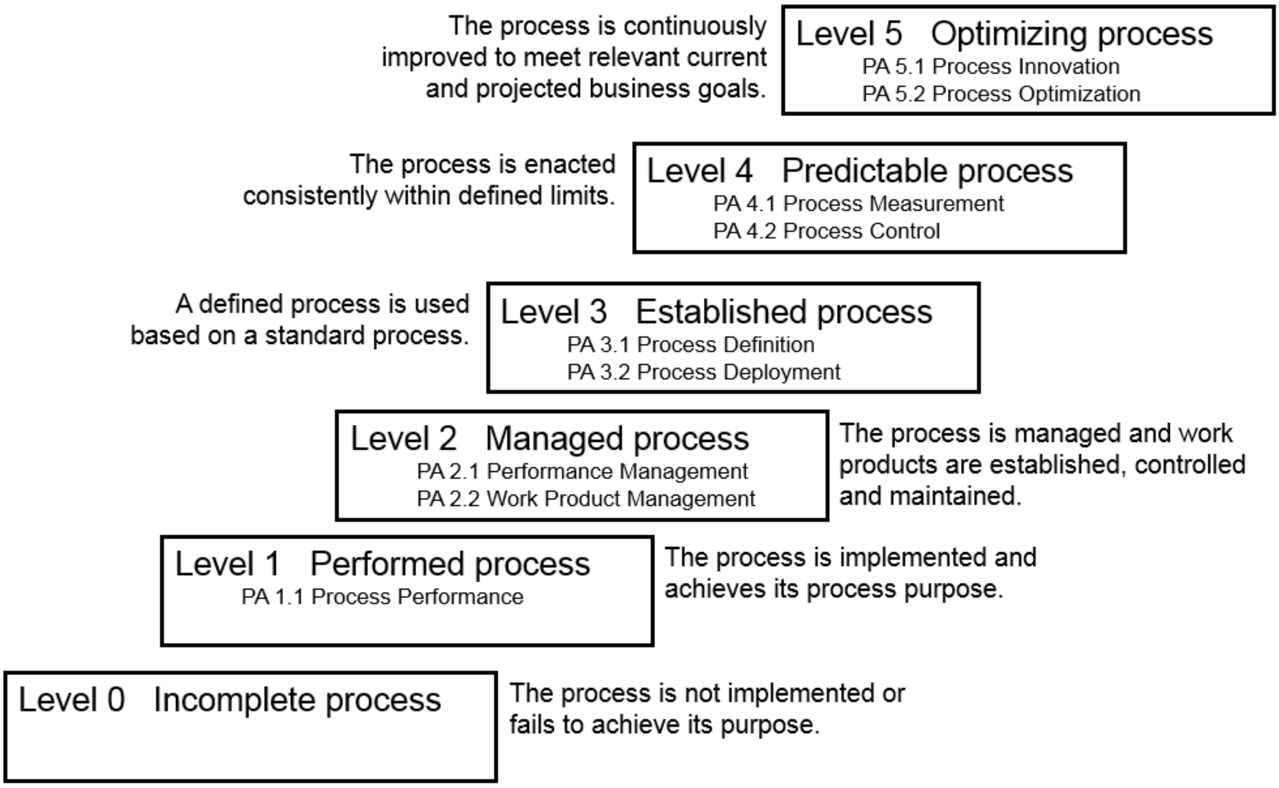
The process is continuously improved to meet relevant current and projected business goals.
Level 5 Optimizing process
PA 5.1 Process Innovation
PA 5.2 Process Optimization
The process is enacted consistently within defined limits.
Level 4 Predictable process
PA 4.1 Process Measurement
PA 4.2 Process Control
A defined process is used based on a standard process.
Level 3 Established process
PA 3.1 Process Definition
PA 3.2 Process Deployment
Level 2 Managed process
PA 2.1 Performance Management
PA 2.2 Work Product Management
The process is managed and work products are established, controlled and maintained.
Level 1 Performed process
PA 1.1 Process Performance
The process is implemented and achieves its process purpose.
Level 0 Incomplete process
The process is not implemented or fails to achieve its purpose.

Figure 1: ISO/IEC 15504 Process Capability Measurement Framework

ISO/IEC 15504 *Capability Levels* and related *Process Attributes* 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). Note that as the risk management professionals often use the terms of "risk tolerance" and "risk appetite" with different meanings, the "risk criteria" term of ISO 31000 might be more commonly understandable by most of the users.

Capability profiles of key business and enabling governance processes are representing "reverse", but well understandable measures of risk appetite as the higher capability levels indicate the more robust risk treatment in supporting the achievement of relevant business objectives. In this term there are no "good" or "bad" capability levels, as they are determined by management decisions keeping in mind the risk treatment costs and benefits together with the implicit and explicit expectations of the key stakeholders.

ISO/IEC 15504 standard provides description of process assessment method providing transparent, reliable and repeatable ratings for those processes which are defined in a conformant way (widely agreed by domain experts). Specific and generic indicators for measuring achievement of capability level attributes are representing well established measures for applicable risk criteria in setting acceptable (tolerable) risk levels.

While the lower capability (1-2) levels give operational insights, the higher (3-5) levels provide organizational contexts for improving process performance. The wider gaps at lower capability levels represent the higher residual risks (effects of uncertainties) after current improvement cycles implemented as planned risk treatment activities.

In order to select those business and enabling governance processes which are relevant for setting risk appetite and improving business performance, **Quantitative Performance Measurement** covering the overall governance structure is needed. By establishing measurable risk criteria in supporting management decisions at all organizational and operational levels, the linkage between the processes based for risk appetite statements (as improvement targets) and specific enterprise goals are set. Most of the metrics applied by Quantitative Performance Measurement, like those related to “Usefulness” and “Efficiency” *generic attributes* [5], are typically not interpretable for the ISO/IEC 15504 process capability levels. These metrics are applicable in business context of the processes by providing tool for defining and/or adapting economically meaningful application practices from recognized control frameworks and well established process reference models as process performance (level 1) indicators.

2. Applicable Governance Objectives and Enabling Processes

The well established and recognized control frameworks and process reference models could be used for implementing and evaluating effective and efficient Enterprise Governance, if only the management established its own governance related objectives. Unfortunately, structures of generic control frameworks and reference models promoted by assurance professional bodies are not easily interpretable by enterprise management for setting their own business’ specific governance objectives.

The **Governance Model for Trusted Businesses** keeps both enterprise management and assurance (e.g. audit) logics in mind by presenting governance processes in line with the specific objectives relevant for the company, together with an exact mapping to processes of control frameworks (reference models) accepted and used by assurance providers for compliance attestation. This approach may contribute to the transition from the traditional control based risk assessment to objectives driven integrated risk management.

The Governance Model aims 11 governance objectives:

Supporting Business Sustainability:	*Supporting Organization’s Internal Control System:*		
✓ **Competitiveness**	✓ **Accountability**	✓ **Commitment**	✓ **Risk Awareness** ✓ **Control Efficiency**
✓ **Exploitability**	✓ **Process Integrity**	✓ **Competency**	
✓ **Satisfaction**	✓ **Accuracy**	✓ **Data Protection**	

Figure 2: Applicable Governance Objectives for Trusted Business

While business sustainability objectives are significant for keeping business operation economically effective and successful, the organization’s internal control objectives have the major focus on how effectively internal control system is enabling achievement of strategic, operational effectiveness, reliability and business process performance related Enterprise Goals. Each governance objective should be determined in context of the specific organizational or operational level by considering the adequate time-horizon.

The different operational and organizational levels have specific targets and time-horizons. At each level the specific “Usefulness” and “Efficiency” goals and measures allow management to see recognized governance and control framework descriptions as enablers instead of compliance requirements. By considering applicability of the “Usefulness” and “Efficiency” metrics, the context and relevance of the governance and control practices selected from the generic frameworks are determined.

Criteria for tolerable level of risks can be established by referring to those business and enabling governance processes and their capability level targets, which are closely related to the relevant enterprise goals. The structure of enterprise goals and how the governance objectives are supporting the achievement of these goals determine the internal contexts of setting capability targets as enterprise-wide risk levels. The structure of enterprise goals and related governance objectives can be presented as follows:

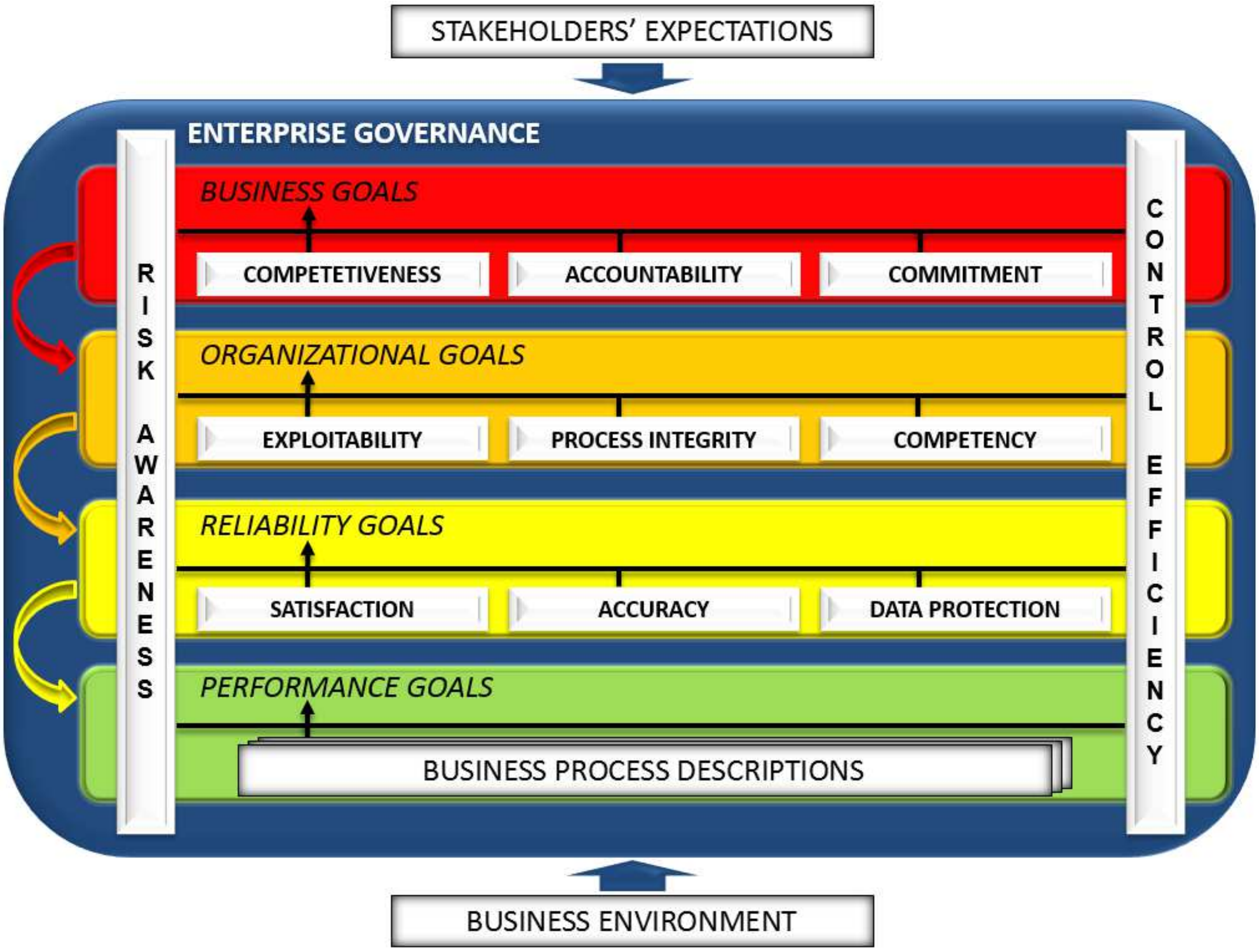

Figure 3: Linking Governance Objectives to Enterprise Goals

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 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.

The Governance Model for Trusted Businesses provides ISO/IEC 15504 conformant process descriptions and application practices for the above mentioned governance objectives enabling achievement of enterprise goals.

The following three governance processes are defined related to business sustainability objectives:

- *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.

Eight processes are defined related to the internal control objectives:

- *Control Risks* – The organization and its staff adequately address risks to the governance objectives 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 business operation.
- *Control Competence* – Sufficient skills and knowledge relevant for the objectives of business operation are available and used.
- *Information Reliability* – Data architecture and disclosure elements relevant for 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 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 business operation, and availability principle.
- *Control Efficiency* – Efficient usage of control resources relevant to the objectives of business operation.

The **Governance Model for Trusted Businesses** provides adaptable application practices for the above listed governance processes by offering suggestions from recognized reference models (COSO, COBIT [6], Enterprise SPICE [7]) and the generally accepted privacy principles. The "Usefulness" and "Efficiency" metrics, the context and relevance for enterprise goals at the given operational and organizational levels should determine what elements from the recognized models should be reasonably followed.

The **Integrated Risk Management Scenarios** are tools for implementing risk management framework integrated with Enterprise Governance. The Integrated Risk Management Scenarios are established by mapping already implemented or newly developed management practices to governance objectives - through company specific enterprise goals. By this way also the compliance and assurance works are aligned with the enterprise specific business objectives and might keep the less meaningful elements of general governance or control frameworks out of scope. By comparing existing practices to those offered by these frameworks, the management and - if requested due to company size or corporate laws - the board might benefit from getting wider professional knowledge and best practice suggestions for improving Enterprise Governance.

3. Implementing Enterprise Goals driven Integrated Risk Management Scenarios

The term of *"scenario"* is used for systematically considering integrated risk management aspects of enterprise governance practices implemented at operational and organizational levels. These considerations are focusing on the customized design of governance objectives, processes and practices enabling the better achievement of the concerning enterprise goals, and the presentation of related risk criteria as management assertions or risk appetite statements. Based on the evaluation of how these risk criteria are fulfilled, the next improvement or correcting actions (risk treatments) are planned and performed. The ISO 31000 standard sets applicable requirements for these risk management activities at organizational and process levels.

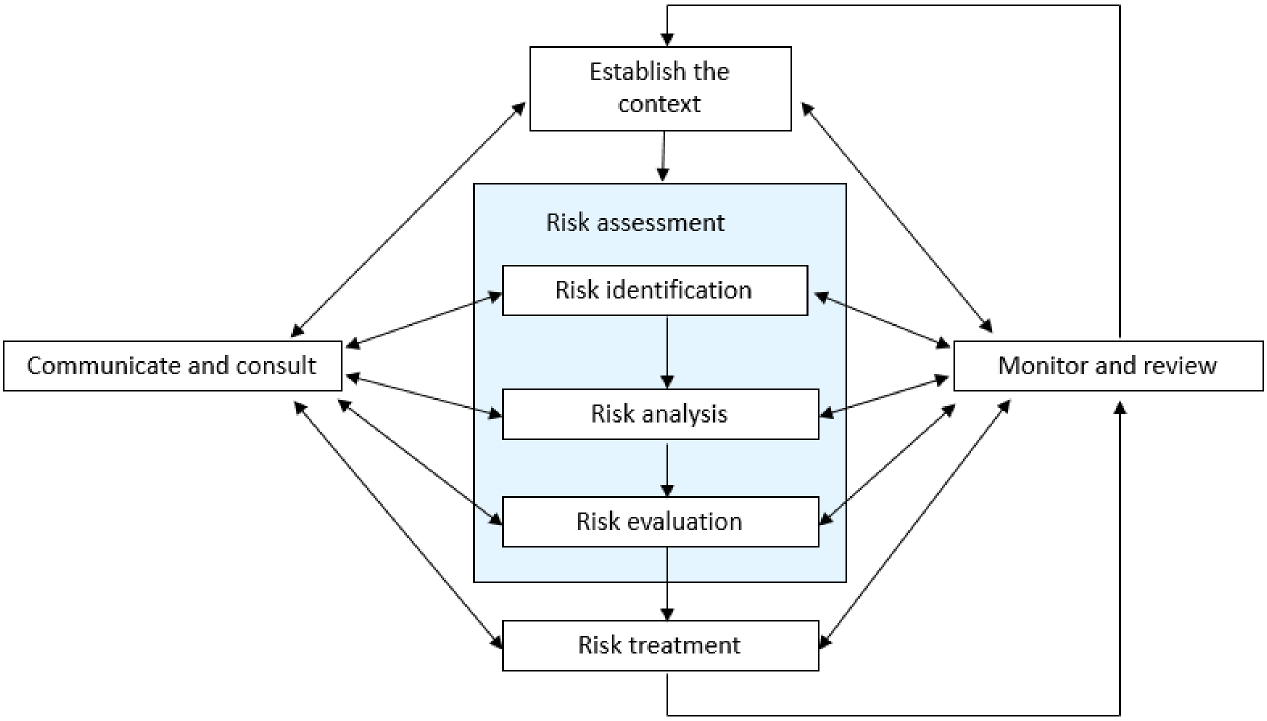

Figure 4: Risk Management Activities at Process Level (ISO 31000 Risk Management Process)

The Enterprise Risk Management framework, if it is well established and maintained, will guide the organization to effectively implement risk management activities integrated into business processes at all relevant organizational and operational levels. In this term effectiveness conclusion should be based on the achievement of the following outcomes (based on ISO 31000):

- The organization has a current, correct and comprehensive understanding of its risks (effects of uncertainties on objectives at all operational and organizational levels).
- All relevant external and internal stakeholders have necessary and sufficient information over organization's tolerable risk levels driving their actions based on their judgement of how the organization's tolerable risk levels effect their own specific objectives.
- The organization's risks are within its risk criteria of tolerable risk levels over periods driven by the nature of objectives and related risk criteria.

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. **Integrated Risk Management Scenarios** are used for determining enterprise framework of managing risks at all operational and organizational levels by implementing risk treatments as process improvement cycles in supporting better business performance.

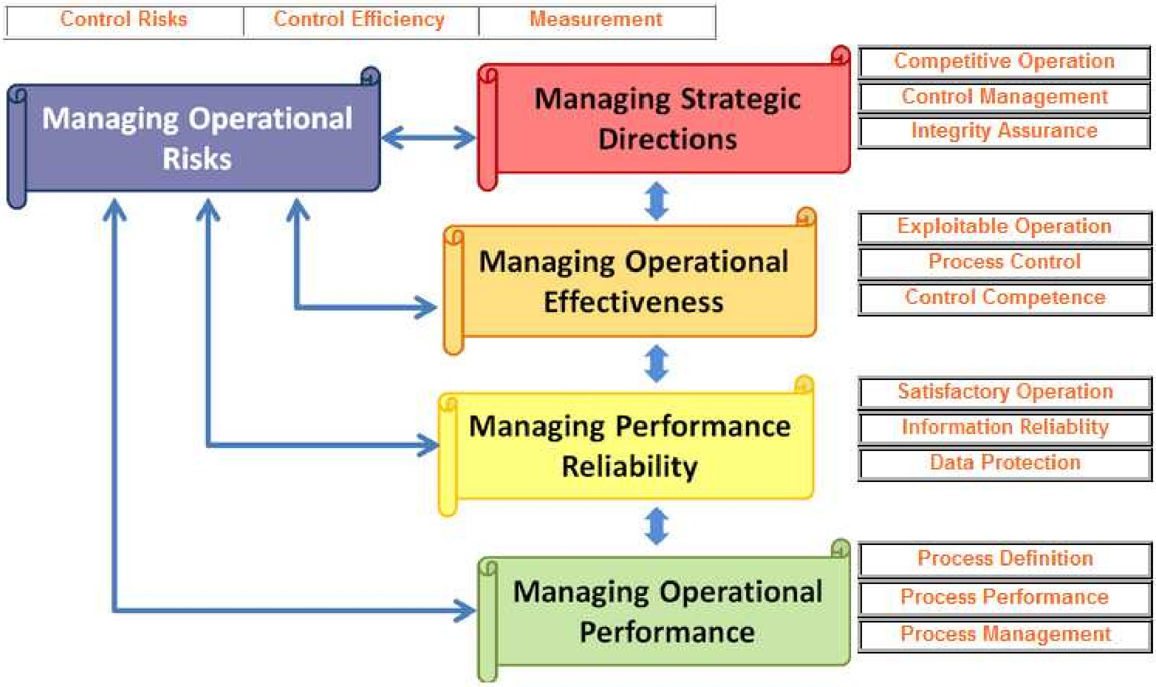

Figure 5: Integrated Risk Management Scenarios and Enabling Governance Practices

The proposed Integrated Risk Management Scenarios are applicable for all types of business entities and they use generic purpose governance frameworks for selecting those processes and practices which enable their business operations to achieve enterprise goals at adequately defined operational and organizational levels.

4. Applying Governance SPICE Assessor Skills

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) based **Governance Capability Assessment** [8] 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 specific 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 application practices selected from the COSO, COBIT and Enterprise SPICE reference models. The governance processes associated with the process attributes defined by ISO/IEC 15504 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 standard (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.

The **Governance Model for Trusted Businesses** and **Governance Capability Assessment** help the executive management and - if it exists - the board to look at compliance issues through customized governance objectives aligned with enterprise specific business goals and stakeholders’ expectations.

The Governance Model for Trusted Businesses provides process descriptions and applicable practices for setting risk criteria over Enterprise Governance assuring achievement of specific enterprise goals according to stakeholders’ needs and expectations. The **Governance SPICE Assessor** skills [9] are required to evaluate these management assertions or risk appetite statements established by Integrated Risk Management Scenarios implemented at organizational and operational levels.

By using the terminology outlined in the **ECQA skills definition model** [10], the skills hierarchy for the job role “Governance SPICE Assessor” has been designed. The skill units and elements cover the relevant “Governance” domain specific knowledge (Governance, Risk and Controls), the principles of the Governance Model for Trusted Businesses (Governance Objectives), the basics of SPICE (Process Assessment) and the mapping of capability levels with Compliance, Reporting, Operations and Strategic objectives (Governance Capability). Next figure also presents the detailed list of the learning elements:

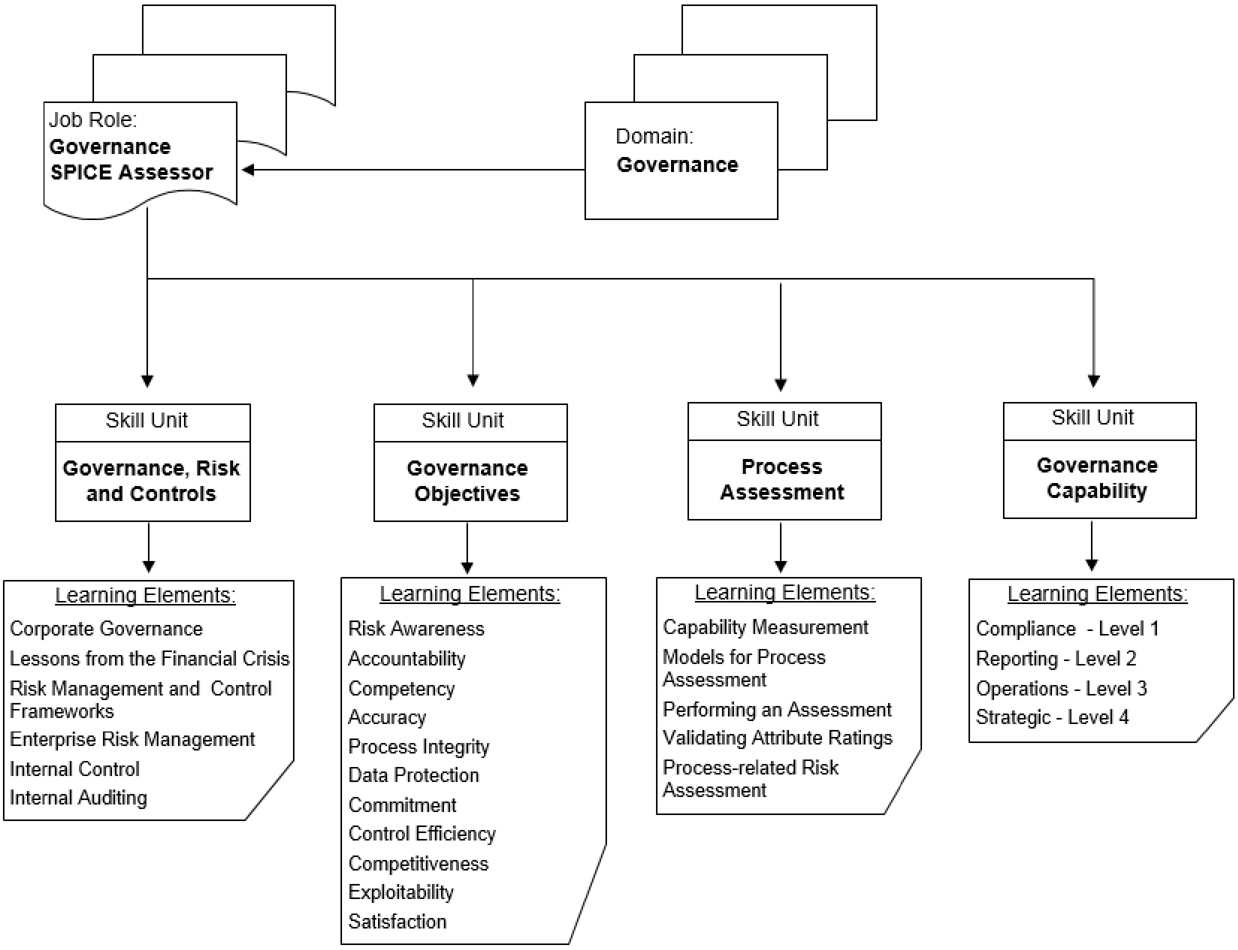

Figure 6: The ECQA certified Governance SPICE Assessor Skill Card

5. Conclusions

The **Integrated Risk 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. Even in the case of SMEs the business environment might have internationally standardized control requirements (like **SOC 1** [11] and **SOC 2** [12]), which should be carefully considered by small business companies providing local services to big firms or 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.

By changing from the traditional *model based compliance* to *enterprise goals driven integrated risk management*, the management assertions (the links between business activities and governance practices) are implemented by applying significantly different scoping approach. The key business processes are viewed as instances of business performance at different operational and organizational levels, so the Integrated Risk Management Scenarios are enhancing the meaning of "compliance" as *in what extent the model based governance/control practices are relevant for really supporting the achievement of enterprise goals within their acceptable tolerance levels*. The proposed Integrated Risk 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 Risk 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 (if exits), 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.

For all the 11 governance objectives the **Governance Model for Trusted Businesses** provides application practices with reference to governance processes offered by recognized reference models (COSO, COBIT, Enterprise SPICE) or generally accepted (e.g. privacy) principles. The full coverage of the governance objectives related processes - by implementing the **Integrated Risk Management Scenarios** lets enterprises to qualify their business units. The qualification process of a business unit's **compliance to its unique governance objectives** - defined by the specific scoping of the governance practices from the Governance Model for Trusted Businesses - should cover all those business processes and information sources, which provide the sufficient evidences for management assertions (risk appetite statements) concerning to the effective and efficient implementation of enterprise risk management scenarios.

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 enabling processes of 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.

Professionals having been acquiring and evidencing their **Governance SPICE Assessor** skills are able to provide unique consulting and assurance services for supporting enterprises in achieving well established business goals and targets at an affordable level of risk treatment costs and effect of uncertainties by assessing and evaluating enterprise governance processes.

6. References

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

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

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

- Internal Control - Integrated Framework (1992, 2013)
- Enterprise Risk Management - Integrated Framework (2004)
- Internal Control over Financial Reporting - Guidance for Smaller Public Companies (2006)
- Enterprise Risk Management - Understanding and Communicating Risk Appetite (2012)

[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
ISO/IEC TR 15504-7:2008 Information technology -- Process assessment -- Part 7: Assessment of organizational maturity
(The ISO/IEC 15504 series of standards is being replaced by the ISO/IEC 33001-99 series of standards.)

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

[6] COBIT - Control Objectives for Information and related Technology,
COBIT 4.1 © 2007 and COBIT 5 © 2012, IT Governance Institute

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

[8] 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

[9] Governance SPICE Assessor and Internal Financial Control Assessor Skill Cards, ECQA Committees, 2011

[10] Rules and Process Steps for Certification of ECQA Job Role, Version: Approved (2011), European Certification and Qualification Association, www.ecqa.org

[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.

7. Author CV

János Ivanyos is the founder of Trusted Business Partners Ltd. providing advisory and qualification services related to governance skills and capability development for those companies which are committed to the trusted business principles by applying best practices of enterprise governance, risk management and internal controls. Formerly he had been a partner and managing director at Memolux Ltd., a Hungarian 70 people in staff accounting and IT service company, for 22 years.

He was graduated as an economist at the Karl Marx University of Economics, Budapest in 1984. He has more than 25 years of experience in IT management, and he has successfully coordinated many technically complex, international (Europe-wide) research and training projects since 1995.

He is associate professor at the Budapest Business School, board member and secretary at the Corporate Governance section of the Hungarian Economic Association, advisory board member at the Enterprise SPICE initiative, and committee leader at the European Certification and Qualification Association. He is author of several papers and proceedings of international conferences (including ECQA, EuroSPI, IIA and ISACA events).