ECQA Governance SPICE Assessor Skills for Evaluating Integrated Risk Management Scenarios

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

Abstract. 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 capability of enterprise governance processes.

Keywords: Governance Capability, ISO/IEC 15504 (SPICE), Enterprise SPICE, COSO, COBIT, ISO 31000 Risk management, Enterprise Risk Management (ERM), Trusted Business

1. Risk Management Principles Supporting 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 all 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 is not really far from applying 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 measurable 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, formalized as Risk Appetite Statements (at strategic level) or Management Assertions (at operational and organizational levels), instead of complying with generic models normally used as simple check-lists by assurance providers (e.g. auditors).

The ISO/IEC 15504 standard [4] based process improvement and capability determination methodology provides a conceptual 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.

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 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 (e.g. auditors) for compliance attestation.

The Governance Model aims 11 governance objectives:

<table>
<thead>
<tr>
<th>Supporting Business Sustainability</th>
<th>Supporting Organization's Internal Control System:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Competitiveness</td>
<td>✔ Accountability</td>
</tr>
<tr>
<td>✔ Exploitability</td>
<td>✔ Process Integrity</td>
</tr>
<tr>
<td>✔ Satisfaction</td>
<td>✔ Accuracy</td>
</tr>
<tr>
<td></td>
<td>✔ Data Protection</td>
</tr>
<tr>
<td></td>
<td>✔ Risk Awareness</td>
</tr>
<tr>
<td></td>
<td>✔ Control Efficiency</td>
</tr>
</tbody>
</table>

Figure 1: 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 governance objectives should be supported by “Usefulness” and “Efficiency” measures and other risk criteria for improving business processes and management activities within the enterprise governance framework.

The Governance Model provides ISO/IEC 15504 conformant process descriptions and application practices for providing assurance over trusted and sustainable business operation.

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 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.

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).

3. **Implementing Enterprise Goals driven Integrated Risk Management scenarios**

The term of “scenario” is used for systematically considering integrated risk management aspects of governance practices implemented at given operational or organizational level. These considerations are focusing on the customized design of governance objectives, processes and practices enabling the 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 describes applicable requirements for these risk management activities at organizational and process levels.
The suggested solution describes how 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 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.

The proposed Integrated Risk Management scenarios are distinguishing different operational and organizational levels having specific targets and time-horizons. At each level “Usefulness” and “Efficiency” goals and measures should be defined allowing management to see recognized professional framework practices as enablers instead of just compliance requirements.

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.

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 [5] 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 selected processes from the COSO, COBIT [6] and Enterprise SPICE [7] 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. Quantitative Performance Measurement covering the overall governance structure is needed for establishing useful risk criteria for supporting management decisions at all organizational and operational levels.
Most of the metrics applied by Quantitative Performance Measurement, like those related to “Usefulness” and “Efficiency” generic attributes [8], 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 base practices as process performance (level 1) indicators. There is no meaning to establish such metrics for the generic practices of higher capability level Process Attributes; however highlighting of the generic attribute metrics of those business or governance practices, which are identified enablers of higher capability level practices for all processes within the scope of the process assessment model, is more than reasonable. Those base practices adapted from control frameworks or reference models as performance (level 1) indicators of a governance process, are applicable to determine risk appetite at operational and organizational levels.

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 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 (risk appetite statements) established by Integrated Risk Management scenarios implemented at different organizational and operational levels.

By using the terminology outlined in the ECQA skills definition model, 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 3: 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 (like SOC 1 [10] and SOC 2 [11]) requirements 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


• Internal Control - Integrated Framework (1992, 2013)
• Enterprise Risk Management - Understanding and Communicating Risk Appetite (2012)

ISO/IEC 15504-2:2003/Cor 1:2004


