BPM-GOSPEL

Governance Capability Assessment
Case Study Handbook

Integrated Assurance Management Scenarios for
Trusted Business Operation

Co-Authors
Project Partners

Status: Name: Date: Signature:
Draft: J. Ivanyos 15.12.2012 n.n. electronically
Reviewed: Project Partnership 23.12.2012 n.n. electronically
Approved: Project Partnership

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Amendment history

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision</th>
<th>Date</th>
<th>Pages</th>
<th>Author</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>25.06.2012</td>
<td>All</td>
<td>JI (Memolux)</td>
<td>Completed Edition</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>15.12.2012</td>
<td>All</td>
<td>JI (Memolux)</td>
<td>Renaming to Integrated Assurance Management</td>
</tr>
</tbody>
</table>

Distribution list

- Project partners
- Project Officer
- External Reviewers

Quality System References

ISO 9001 compliant planning and review processes are applied.
Contents

1. INTRODUCTION ................................................................. 7
   1.1 OBJECTIVE ........................................................................... 7
   1.2 PURPOSE OF THE DELIVERABLE ........................................... 7
   1.3 SCOPE OF THE DELIVERABLE ............................................... 7
   1.4 THE BPM-GOSPEL PROJECT .................................................. 8
   1.5 THE BPM-GOSPEL PROJECT PARTNERSHIP .............................. 9
   1.6 ACRONYMS AND DEFINITIONS USED .................................... 10
   1.7 REFERENCES ........................................................................ 11

2. APPLIED PRINCIPLES .............................................................. 12
   2.1 GOVERNANCE PRINCIPLES IN STRENGTHENING BUSINESS 
       TRUST AND SUSTAINABILITY ................................................. 12
   2.2 ENTERPRISE GOALS driven INTEGRATED ASSURANCE MANAGEMENT 
       SCENARIOS ......................................................................... 13
   2.3 GOVERNANCE OBJECTIVES OF THE GOVERNANCE MODEL FOR Trusted 
       BUSINESSES ..................................................................... 15
   2.4 GOVERNANCE CAPABILITY ASSESSMENT .............................. 16
   2.5 LINKING GOVERNANCE OBJECTIVES TO ENTERPRISE GOALS & MEASURES .............................. 18

3. THE BASELINE BUSINESS CASE ............................................. 19
   3.1 NEED FOR ASSURANCE OF SERVICE ORGANIZATION’S CONTROL .......... 19
   3.2 BACKGROUND INFORMATION FOR THE BUSINESS CASE ................. 21
   3.3 MAPPING THE BUSINESS PROCESS TO GOVERNANCE PRACTICES ............. 22
   3.4 IMPLEMENTING THE OUTSOURCING BUSINESS PROCESS IN STAGES PROCESS MANAGEMENT SYSTEM ... 24
   3.5 USING COMPLIANCE WORKBENCH OF STAGES .............................. 28
   3.6 EXTERNAL VALIDATION BY CAPABILITY ADVISER TOOL .................... 32

4. INTEGRATED ASSURANCE MANAGEMENT SCENARIOS SUPPORTING ENTERPRISE GOVERNANCE .................. 34
   4.1 COMMENTS for IMPLEMENTING INTEGRATED ASSURANCE MANAGEMENT SCENARIOS .......................... 34
   4.2 MANAGING OPERATIONAL PERFORMANCE .................................. 38
      4.2.1 Context and Specific Learning Objectives of Managing Operational Performance .................. 38
      4.2.2 Selecting the Scope of the Management Assertions for Managing Operational Performance .......... 42
      4.2.3 Defining Process Outcomes for Managing Operational Performance ................................. 45
      4.2.4 Applying generic - level 2 - Managed capability indicators as risk criteria for Performance Goals .... 48
   4.3 MANAGING PERFORMANCE RELIABILITY .................................. 52
      4.3.1 Context and Specific Learning Objectives of Managing Performance Reliability ..................... 52
      4.3.2 Selecting the Scope of the Management Assertions for Managing Performance Reliability .......... 56
      4.3.3 Applying Management Assertions for Managing Performance Reliability ............................. 61
      4.3.4 Selecting specific application practices as risk criteria for Reliability Goals ............................. 63
   4.4 MANAGING OPERATIONAL EFFECTIVENESS ................................ 69
      4.4.1 Context and Specific Learning Objectives of Managing Operational Effectiveness .................... 69
      4.4.2 Selecting the Scope of the Management Assertions for Managing Operational Effectiveness .......... 73
      4.4.3 Applying Management Assertions for Managing Operational Effectiveness ............................ 78
      4.4.4 Selecting specific application practices as risk criteria for Operational Effectiveness Goals ........ 80
   4.5 MANAGING STRATEGIC DIRECTIONS ....................................... 90
      4.5.1 Context and Specific Learning Objectives of Managing Strategic Directions ............................ 90
      4.5.2 Selecting the Scope of the Management Assertions for Managing Strategic Directions ............... 94
      4.5.3 Applying Management Assertions for Managing Strategic Directions ..................................... 99
      4.5.4 Selecting specific application practices as risk criteria for Strategic Directions ...................... 101
   4.6 MANAGING OPERATIONAL RISKS ........................................... 108
      4.6.1 Context and Specific Learning Objectives of Managing Operational Risks ............................. 108

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of 
the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
4.6.2 Selecting the Scope of the Management Assertions for Managing Operational Risks .................. 112
4.6.3 Applying Management Assertions for Managing Operational Risks ........................................... 117
4.6.4 Selecting specific application practices as risk criteria for Managing Operational Risks .............. 119
4.7 ASSURANCE EXAMPLES ............................................................................................................. 131
4.7.1 Assurance on a Business Process at Managed level ................................................................. 131
4.7.2 Assurance on a Governance Process ......................................................................................... 137
Figures

Figure 1: Enterprise Goals driven Integrated Assurance Management scenarios .................................................. 13
Figure 2: Governance Objectives for Trusted Businesses .................................................................................. 15
Figure 3: Dimensions of Governance Capability Assessment ........................................................................ 16
Figure 4: Linking Governance Objectives to Enterprise Goals & Measures ..................................................... 18
Figure 5: Supervision layer of the Monthly Payroll Calculation business process ........................................... 24
Figure 6: Activity layer for Client's Data Takeover process element .................................................................. 25
Figure 7: Scope selection from the Governance Model for Trusted Businesses ................................................. 29
Figure 8: Mapping business process against the scope ................................................................................... 29
Figure 9: Rating a lower level governance objective ....................................................................................... 30
Figure 10: Checking relevant assertions and the linked evidence sources during rating ................................... 30
Figure 11: Evidence table viewed in Capability Adviser .................................................................................. 33
Figure 12: Rating and commenting compliance by Capability Adviser .............................................................. 33
Figure 13: Role of the Managing Operational Performance scenario in Enterprise Governance ..................... 38
Figure 14: Four point ordinal scale for evaluating the achievement of process attribute .................................. 47
Figure 15: Role of the Managing Performance Reliability scenario in Enterprise Governance ....................... 52
Figure 16: Role of the Managing Operational Effectiveness scenario in Enterprise Governance..................... 69
Figure 17: Role of the Managing Strategic Directions scenario in Enterprise Governance ............................ 90
Figure 18: Role of the Managing Operational Risks scenario in Enterprise Governance .............................. 108
Figure 19: Control Efficiency considerations in context of risk treatment costs ............................................. 116
Tables

Table 1: Mapping of the Monthly Payroll Calculation activities to Accuracy governance objective
Table 2: Description for the Supervision layer of the Monthly Payroll Calculation business process
Table 3: Description for the Activity layer for Client's Data Takeover process element
Table 4: Assertion for involving IT, professional and process assessment support for client's data takeover
Table 5: Operational Performance related risk areas
Table 6: Outcomes of Monthly Payroll Calculation process with sample metrics
Table 7: Mapping Managed Process Capability with enabling Governance Practices
Table 8: Satisfaction related risk areas
Table 9: Accuracy related risk areas
Table 10: Data Protection related risk areas
Table 11: Application Practices of Satisfactory Operation with possible metrics
Table 12: Exploitability related risk areas
Table 13: Process Integrity related risk areas
Table 14: Competency related risk areas
Table 15: Application Practices of Exploitable Operation with possible metrics
Table 16: Competitiveness related risk areas
Table 17: Accountability related risk areas
Table 18: Commitment related risk areas
Table 19: Application Practices of Competitive Operation with possible metrics
Table 20: Risk Awareness related risk areas
Table 21: Control Efficiency related risk areas
Table 22: Application Practices of Control Risks with possible metrics
Table 23: Application Practices of Control Efficiency with possible metrics
Table 24: Ratings of the Monthly Payroll Calculation process against - level 2 - Managed capability
Table 25: Ratings of the Satisfactory Operation and its enabling Governance Practices

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, 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 deliverable is to provide a handbook for the Governance Capability Assessor trainings by presenting how the Governance Capability Assessor skills are applicable to implement Integrated Assurance Management scenarios in sample business environment of an outsourcing service company. These Integrated Assurance Management scenarios take the governance objectives of the Governance Model for Trusted Businesses into the context of the operational and organizational levels and their specific business goals.

1.2 Purpose of the Deliverable

The deliverable presents:

- the principles applied in the case study
- the baseline business case enhanced by the Integrated Assurance Management scenarios
- the Managing Operational Performance scenario
- the Managing Performance Reliability scenario
- the Managing Operational Effectiveness scenario
- the Managing Strategic Directions scenario
- the Managing Operational Risks scenario
- the assurance examples

by referring to the following public deliverables of the BPM-GOSPEL project:

- Governance Model for Trusted Business [1]

1.3 Scope of the Deliverable

The deliverable contains

- A chapter about principles applied in the case study
- A chapter about the baseline business case
- A chapter covering 5 Integrated Assurance Management scenarios
- A chapter for assurance examples

Presentation of the 5 scenarios (in chapter 4) follows similar structure and contains some overlapping information allowing even separate usage of any scenario as specific business case for implementing enterprise goals driven integrated assurance management.

The deliverable does not contain:

- the full version of the Integrated Governance SPICE Assessor skill card
- the Governance Model for Trusted Business
- the Business Case Implementation Report
- the detailed technical manuals and user guides of the systems used
- the test and evaluation reports.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
1.4 The BPM-GOSPEL Project

The objective of the BPM-GOSPEL - Business Process Modelling for Governance SPICE and Internal Financial Control - project (2010-2013) is the transfer of the already proved innovation - multiple model based compliance workbench tool for improving governance capability of business processes [3] - from Germany to Hungary, where the existing results of IA-Manager (2005-2007) and MONTIFIC (2008-2010) training development projects are further enriched by Integrated Assurance Management scenarios using 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 Integrated Assurance Management 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 implemented by the baseline business case are presented below:

---

**Figure 1: Implemented layers of Business Process Modelling for the BPM-GOSPEL baseline business case**

The Governance Model for Trusted Business - a publicly available deliverable of the BPM-GOSPEL project - provides reference processes for mapping operational and organizational management practices to control compliance and audit management objectives. The business case baseline has been implemented through the above BPM layers by the “Stages” platform with interfaces to workflow management (Adamas) and audit management (Capability Adviser) tools.

Adding business goals driven Integrated Assurance Management scenarios to training materials (like on 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" has been used as a multi-layer BPM tool for presenting business baseline case selected for “coaching” of governance objectives though practical implementation of the processes and practices of the Governance Model for Trusted Businesses for private and public sector companies by referring to internationally recognized control frameworks like COSO [4], COBIT [5], Enterprise SPICE [6] and related process assessment (SPICE) approach [7] used by Governance Capability Assessment [8].
1.5 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
1.6 Acronyms and Definitions Used

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and related Technology</td>
</tr>
<tr>
<td>COSO</td>
<td>COSO Internal Control – Integrated Framework</td>
</tr>
<tr>
<td>COSO ERM</td>
<td>COSO Enterprise Risk Management — Integrated Framework</td>
</tr>
<tr>
<td>ESPICE</td>
<td>Enterprise SPICE</td>
</tr>
<tr>
<td>GAPP</td>
<td>Generally Accepted Privacy Principles</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>PA</td>
<td>Process Attribute</td>
</tr>
<tr>
<td>SOC</td>
<td>Service Organization’s Control</td>
</tr>
<tr>
<td>SPICE</td>
<td>Process Improvement and Capability Determination</td>
</tr>
</tbody>
</table>
1.7 References


   - Internal Control — Integrated Framework (1992)


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


[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.


This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
2. Applied Principles

2.1 Governance Principles in Strengthening Business Trust and Sustainability

Corporate 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.

It is important to all economic and social partners, that the enterprise governance milieu - by keeping in mind all the needs and requirements of the markets’ demand and supply relations, the regulatory environment enforcing public societal interests, and the company stakeholders’ expectations together supports the optimal framework of risk taking in establishing and maintaining long term and fruitful business relationships necessary for the sustainable development. Therefore it is desirable for the achievement of a standard level of business trust that those governance principles and enabling practices which are commonly interpretable and observable by all types of economic entities will be as widely as possible acquainted and also applied according to the specific business conditions. Implicitly the enterprise has the more and the more types of business relationships and stakeholders, the more important is the control and transparency of its governance system supporting business trust. Nevertheless, the successful conformity to governance requirements and the credible presentation of the achieved results are equally important to the entities either in start-up, growing or matured phases - independently from size, industry sector or ownership types.

For publicly listed companies, the regulators or supervision authorities request compliance to the local corporate governance codes or recommendations. In Europe the “comply or explain” type disclosures are generally accepted, however stakeholders would be more happy with wider transparency of how the fulfilled compliance objectives are achieved instead of just receiving short explanations of why some compliance requirements are missed or managed in different than the recommended way.

Small or Medium sized Enterprises are typically not requested to disclose conformity statements. However if their products or services are embedded into their customers’ production lines, the necessary technical, quality and financial indemnity insurance requirements and the validation processes are established and maintained within formal supply chain management. In outsourcing business even the small entities might be asked to provide independent audit reports for Service Organization’s Control. Funding agencies, investors and financial institutions can rate their potential SME clients not only based on the historical financial figures, in optimal business environment the “soft” organizational management factors and company goodwill are also evaluated and important for decision making. 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 aligned with their own business goals and environment. Most of the given governance processes and necessary practices don’t need to be implemented in different or new way from existing company management practices by linking existing - already proofed - management practices to generic governance objectives for better achieving transparency to external stakeholders.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
2.2 **Enterprise Goals driven Integrated Assurance Management scenarios**

The suggested solution describes how Integrated Assurance Management scenarios can be established by 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.

![Diagram](image)

**Figure 1: 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 allowing management to see recognized professional framework practices as enablers instead of just compliance requirements. The following Integrated Assurance Management scenarios are presented in this case study handbook:
• 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.

The proposed Integrated Assurance 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.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
2.3 Governance Objectives of the Governance Model for Trusted Businesses

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 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 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></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: Governance Objectives for Trusted Businesses

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.
2.4 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) 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.

![Measurement Framework](Image)

By using Governance Capability concept in customization of governance objectives, the management is able to present management assertions in alignment with both business specific and generic (e.g. regulatory) requirements. These assertions are linking business activities to governance practices within the applied capability assessment model supporting both the implementation of the Enterprise Governance Framework and its internal and external evaluation.
The term of “Governance Capability Assessment” is used in context of Governance, Risk Management and Internal Control processes based on different concepts:

- Corporate Governance Principles and Codes (OECD, etc.)
- 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)

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 — such as other models like Enterprise SPICE — are applicable to set up Process Reference Models in compliance with ISO/IEC 15504-2 requirements.

The selected processes from the COSO, COBIT and the Enterprise SPICE reference models 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 [9]. 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 [10], 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.
2.5 Linking Governance Objectives to Enterprise Goals & Measures

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:

![Diagram of Governance Model](image)

Figure 4: Linking Governance Objectives to Enterprise Goals & Measures

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) is used to evaluate these management assertions established by Integrated Assurance Management scenarios implemented at different organizational and operational levels.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
3. The Baseline Business Case

3.1 Need for Assurance of Service Organization’s Control

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 so called Service Organization’s Control (SOC) reports [11], [12] provide user management with the information they need about the service organization’s controls to help assessing and addressing 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 are specifically intended to meet the needs of entities that use service organizations (user entities) and the certified professionals 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.

The SOC 1 related international standards (like SSAE 16 or ISAE 3402) require 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.

The framework for documenting a service organization’s system for purposes of SOC 1 engagement should include a comprehensive discussion of the following components:

- 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

Management of the service organization must also produce a “written assertion” for purposes of SOC 1 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 were operating effectively.

In a SOC 2 engagement, management of the service organization selects the Trust Services Principles [13] 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.

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 (GAPP) issued jointly by the AICPA and the Canadian Institute of Chartered Accountants.

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 an external auditor 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.

The Governance Model for Trusted Businesses offers sufficient set of practices to determine the enterprise specific control objectives. The service organization 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 considering specific business objectives and real expectations of the business environment). This decision is a clear message to all stakeholders, including user entities and all potential customers, that which operational risks are planned to be mitigated by the service organization management, and which risks remain unattended.

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 the “Stages Trusted Business Edition” 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.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
3.2 **Background Information for the Business Case**

Memolux Ltd. is a Hungarian privately owned 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 for 3 years. 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.

The 20 people staffed Payroll Department has been using in-house developed web-based payroll system for payroll related data maintenance, calculation and reporting for about 100 current clients since year of 2000. The system provides many client-specific interfaces to banking systems and management information systems (like SAP) used in Hungary or world-wide. The software development unit has been participating in European process improvement experiments for decades and maintaining ISO 9001 compliant quality controls.

In 2011 the **ADAMAS work-flow management system** was tested for supporting management controls over the huge number of parallel payroll processing cycles. At first the monthly payroll calculation process was modelled and implemented for starting trials. The ADAMAS system as a work-flow management tool has also the role of providing evidences for management assertions of process-level service organization’s controls.

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 is 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.

**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.

The audit tool in this case is the **Capability Adviser platform**, which allows looking at the business processes and business units through the glance of the recognized reference models’ perspectives. By using Stages process modelling platform in between the evidence pool (work-flow management) and the governance capability assessment tool, the audit work can be transparently fastened by getting evidences directly from where the business processes have been performed, and by gaining better understanding of management’s risk assessment and risk taking approach necessary for judgements of control design effectiveness.

---

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
3.3 Mapping the Business Process to Governance Practices

By mapping the core Monthly Payroll Calculation business process activities with for example the Accuracy objective related governance practices, the company management sets assertions for the business operation in a specific manner, which is adequate to the management’s risk taking behaviour and decisions related to potential inconsistency in payroll processing data architecture and disclosure elements. Of course, the Accuracy objective related governance practices can be also applied by other business processes within a payroll service, so these assertions might be closely linked with others e.g. defined for in-house software development and IT infrastructure management.

The baseline business case modelling and compliance management example (in chapter 3.4-3.6) presents how the Accuracy governance objective related assertions are set by the company management for Monthly Payroll Calculation business process. Please note, that there is not a general requirement that each business activity should be linked to all governance practices related to the governance objective offered by the Governance Model. Normally the implementation instances of the selected set of governance practices evidenced by performed business processes are investigated as enablers of the concerning governance outcome requirement. However this case was used for baseline process modelling.

This baseline process modelling and compliance management example points 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 (as presented in chapter 4), which are applying the model/standard 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.

The next table presents the sample mapping of the Monthly Payroll Calculation activities to Accuracy governance objective related COSO and COBIT control objectives, which was used for the baseline process modelling and compliance management.
<table>
<thead>
<tr>
<th>Activities of the Monthly Payroll Calculation Business Process</th>
<th>COBIT 4.1 PO2 Satisfy the business requirement of being agile in responding to requirements; provide reliable, consistent information, and seamlessly integrate applications into business processes (COBIT 4.1 Define the Information Architecture)</th>
<th>IFC.IC.FRI. 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. (COBIT Financial Reporting Information)</th>
<th>IFC.IC.IC. 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. (COSO Internal Control Information)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO2.1 Create and maintain enterprise information model</td>
<td>using BPM tool for description of payroll cycle planning and preparation</td>
<td>researching client’s satisfaction and requests regarding communication methods and tools</td>
<td>applying documented control requirements for payroll cycle planning</td>
</tr>
<tr>
<td>PO2.2 Create and maintain enterprise data dictionary (ies)</td>
<td>implementing regulatory and client’s requirements</td>
<td>researching client’s satisfaction and requests regarding communication methods and tools</td>
<td>involving IT, professional and process assessment support for client’s data takeover requirements</td>
</tr>
<tr>
<td>PO2.3 Establish and maintain data classification scheme</td>
<td>implementing regulatory and client’s requirements</td>
<td>implementing regulatory and client’s requirements</td>
<td>involving IT, professional and process assessment support for payroll cycle planning</td>
</tr>
<tr>
<td>PO2.4 Manage data integrity</td>
<td>implementing regulatory and client’s requirements</td>
<td>implementing regulatory and client’s requirements</td>
<td>involving IT, professional and process assessment support for payroll cycle planning</td>
</tr>
<tr>
<td>IFIC.FRI.BP1 Use Matrices to Detail Information Flows</td>
<td>keeping data security and consistency by opening new payroll cycle</td>
<td>keeping information takeover rules</td>
<td>applying documented control requirements for payroll cycle planning</td>
</tr>
<tr>
<td>IFIC.FRI.BP2 Obtain Information from External Sources</td>
<td>using BPM tool for description of payroll cycle planning and preparation</td>
<td>using BPM tool for description of client’s data takeover</td>
<td>applying documented control requirements for payroll cycle planning</td>
</tr>
<tr>
<td>IFIC.FRI.BP3 Meet with Personnel from Other Business Area</td>
<td>researching client’s satisfaction and requests regarding communication methods and tools</td>
<td>researching client’s satisfaction and requests regarding communication methods and tools</td>
<td>applying documented control requirements for client’s data takeover requirements</td>
</tr>
<tr>
<td>IFC.IC.BP1 Develop and Maintain Internal Control Information Maps</td>
<td>applying documented control requirements for payroll data processing</td>
<td>applying documented control requirements for data processing</td>
<td>involving IT, professional and process assessment support for data processing</td>
</tr>
<tr>
<td>IFC.IC.BP2 Identify Internal Control Information through Discussion</td>
<td>applying documented control requirements for payroll data processing</td>
<td>applying documented control requirements for data processing</td>
<td>involving IT, professional and process assessment support for data processing</td>
</tr>
</tbody>
</table>

Payroll Cycle Planning
- Implementing regulatory and client’s requirements
- Implementing regulatory and client’s requirements
- Implementing regulatory and client’s requirements
- Keeping data security and consistency by opening new payroll cycle
- Using BPM tool for description of payroll cycle planning and preparation
- Researching client’s satisfaction and requests and regulatory changes for payroll processing
- Applying IT, professional and process assessment support for payroll cycle planning
- Applying documented control requirements for payroll cycle planning

Receive Client’s Data
- Using agreed communication methods and tools
- Using agreed communication methods and tools
- Using agreed communication methods and tools
- Keeping information takeover rules
- Using BPM tool for description of client’s data takeover
- Researching client’s satisfaction and requests regarding communication methods and tools
- Applying IT, professional and process assessment support for client’s data takeover requirements
- Applying documented control requirements for client’s data takeover requirements

Data Processing
- Using in-house developed and tested IT system with verified parameters in controlled environment
- Using in-house developed and tested IT system with verified parameters in controlled environment
- Using in-house developed and tested IT system with verified parameters in controlled environment
- Using BPM tool for description of input data control and processing
- Using BPM tool for description of input data control and processing
- Using BPM tool for description of input data control and processing
- Researching new regulatory and client’s requirements for data processing
- Applying documented control requirements for payroll data processing

Processing Control
- Using IT system (security and event) logs ensuring automated process controls
- Using IT system (security and event) logs ensuring automated process controls
- Using IT system (security and event) logs ensuring automated process controls
- Using BPM tool for description of controlling payroll process
- Identifying possible malfunctions based on external cases and client’s feedback
- Applying documented control requirements for payroll calculation process
- Applying documented control requirements for payroll calculation process

Payroll Output Submission
- Using regulatory and agreed output submission methods and tools
- Using regulatory and agreed output submission methods and tools
- Using regulatory and agreed output submission methods and tools
- Keeping completeness, delivery and formatting requirements, acknowledgement of reception
- Using BPM tool for description of payroll output submission
- Researching regulatory and client’s requirements regarding output submission methods and tools
- Applying documented control requirements for payroll output submission requirements
- Applying documented control requirements for payroll output submission requirements

Reporting and Documenting
- Using regulatory and agreed reporting and archiving formats, methods and tools
- Using regulatory and agreed reporting and archiving formats, methods and tools
- Using regulatory and agreed reporting and archiving formats, methods and tools
- Using BPM tool for description of reporting and archiving methods and tools
- Researching new regulatory and client’s requirements regarding reporting and archiving methods and tools
- Applying documented control requirements for reporting and archiving methods and tools
- Applying documented control requirements for reporting and archiving methods and tools

Table 1: Mapping of the Monthly Payroll Calculation activities to Accuracy governance objective

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
3.4 Implementing the Outsourcing Business Process in Stages Process Management System

“Stages for Trusted Business Edition” tool enables professionals to define and enact business processes, control their standard compliance to governance models and measure process performance. This efficiently stabilizes the foundations for high governance capability in complex corporate business environments.

The key idea behind the “Stages” process management system is to bring process theory and business practices together. Stages platform is optimized for complex but creativity-driven processes and integrates with a large number of tools. It focuses on the end users of processes and provides them with easy access to process descriptions, allowing them to understand both transparent end-to-end processes and role-centric process details.

“Stages for Trusted Business Edition” contains the preconfigured Governance Model for Trusted Businesses, as a reference model for compliance related activities. This part presents how the Monthly Payroll Calculation business process is implemented and used for setting up compliance workbench with the Accuracy objective driven Information Reliability process of the Governance Model.

Implementation starts with defining multiple level activity layers. Within the process definition at first the supervision (by operational management) layer is set up. This layer presents the operational management’s high level supervision view of the process:

Figure 5: Supervision layer of the Monthly Payroll Calculation business process
Description
Supervision and execution of the regular business process performing payroll calculations based on clients’ provided monthly data and regulatory requirements as an outsourcing service. This process consists of the following activities (and assertion):

- 1. Payroll Cycle Planning (...)
- 2. Receive Client's Data (...)
- 3. Data Processing (...)
- 4. Processing Control (...)
- 5. Payroll Outputs Submission (...)
- 6. Reporting and Documenting (...)
- Payroll Cycle Supervision

Inputs from other Processes
- SLA
- Additional Data for Tax Return

Outputs for other Processes
- Payroll Cycle Performance Report
- Non-compliance Report
- Payroll Cycle Control Summary Report

Table 2: Description for the Supervision layer of the Monthly Payroll Calculation business process

At this layer, there is a simple presentation of the main activities of the Monthly Payroll Calculation process with their interdependences and relevant (supervision) assertion, the key inputs and outputs related to the external (Service Level Management) process and to the workflow management system. The workflow schedule and logs provide technical means for management to effectively supervise a Monthly Payroll Calculation process instance and to act immediately if an activity delays or deviation occurs.

Each of the Monthly Payroll Calculation activities has also a more detailed description including roles, work products and reference to the assertions defined for this process element, like in the sample case of Client's Data Takeover.

Figure 6: Activity layer for Client's Data Takeover process element

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
### Roles
- **Responsible:** Payroll Clerk
- **Support:** IT contact
- **Inform:** Payroll Controller, Payroll Operation Manager, Authorities

### Inputs
- Monthly Timesheets
- Ad hoc Payments
- Monthly Sick-leaving Documents
- Input Data Issues
- Employments' Data Modification
- Payroll System

### Outputs
- Sick Leave Data
- Employment Change Report
- Missed Deadline Report
- Filed Payroll Information
- Next Month Data Modification Request
- Immediate Data Modification Request
- Payroll System

### Inputs from other Processes

### Outputs for other Processes

### Description
Standard activity for collecting and recording clients' monthly payroll information based on agreed data-handling rules.

This activity has the following activities:

- Assertion for applying documented control requirements for client's data takeover requirements
- Assertion for involving IT, professional and process assessment support for client's data takeover
- Assertion for keeping client's data takeover rules
- Assertion for researching client’s satisfaction and requests regarding communication methods and tools
- Assertion for using agreed communication methods and tools
- Assertion for using agreed data classification scheme
- Assertion for using agreed data dictionaries
- Assertion for using BPM tool for description of client's data takeover

### Table 3: Description for the Activity layer for Client's Data Takeover process element

This sub-layer presents the operational staff’s view on the business process activities extended with order links to other staff level activities and activity specific inputs and outputs. The business process activities should be performed by keeping requirements set by the related assertions (derived from the governance objectives).

Next example is the “Assertion for involving IT, professional and process assessment support for client’s data takeover”:
<table>
<thead>
<tr>
<th>Governance Assignment</th>
<th>% within Assignment</th>
<th>Risk Area</th>
<th>Control</th>
<th>Entity-level/Process-level</th>
<th>Preventive/Detective</th>
<th>Manual/Automatic</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFC.IC.FRI.BP3 Meet with Personnel from Other Business Area</td>
<td>15%</td>
<td>Non-compliance with rules and regulations are not detected in time</td>
<td>Regular meetings with IT, professional and process assessment support.</td>
<td>Entity-level</td>
<td>Preventive</td>
<td>Manual</td>
</tr>
<tr>
<td>IFC.IC.ICI.BP2 Identify Internal Control Information through Discussion</td>
<td>15%</td>
<td>Availability and quality of control information are not sufficient</td>
<td>Regular meetings with IT, professional and process assessment support.</td>
<td>Entity-level</td>
<td>Preventive and Detective</td>
<td>Manual</td>
</tr>
</tbody>
</table>

Compliance Mappings
Reference mappings to Governance Model for Trusted Businesses V2:


Table 4: Assertion for involving IT, professional and process assessment support for client’s data takeover

The description of the assertion contains reference to the assigned governance objective, weight within assessment scope, mitigated risk area, control description and features, and might have html link to evidence pool.

The compliance mappings show how this assertion is linked to one or more governance objectives.

In the following part we present how the activities, assertions, inputs and outputs can be mapped to the Governance Model elements by using Compliance Workbench functionalities of the Stages.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
3.5 Using Compliance Workbench of Stages

In order to gauge the quality of your business processes, a method is needed to evaluate and quantify them. The evaluation must fulfill criteria with respect to objectivity, reproducibility and comparability, as only then is the evaluation meaningful. In order to achieve such an objective process evaluation, your business processes should be mapped against one or more reference models (e.g. maturity or capability models developed as a quality gage by industry and standardization committees, standards or even in-house standards within an organization). In our case, the business process is mapped to the Accuracy objective related elements (base practices) of the Governance Model for Trusted Businesses.

In order to function as a gage for the processes defined in Stages, reference models must likewise be available in Stages. In order to map processes against reference models, the following steps are necessary:

1. Create a reference model in Stages
2. Assign the process in Stages to the relevant reference model
3. Assign elements from your own process model to the elements of the reference model

By mapping your business process against elements of one or more reference models, you can obtain an evaluation overview that makes visible any deviations as well as the necessary corrective action for improving quality.

Reference models need to be available within Stages in order to be able to map processes against a reference model. These reference models may either be generated from existing processes implemented by Stages or they may be imported from external sources.

In order to map existing processes against reference models that have been set up, the Compliance Workbench makes the following functions available:

- Assign reference models and scopes. This function allows you to create the connection between the process which needs to undergo a quality inspection and the reference model that is to serve as the gage.
- Assign reference elements. This function allows you to assign the relevant elements of the reference model to the elements of the process to be checked.
- Perform Gap Analysis. This function allows you to uncover any deviations between the process and the reference model.
- Generate PIID. This function allows you to generate an Excel table with the information relating to the mapping of the process against the reference model.

The definition of a scope in a reference model allows only the required scope to be selected from the entire reference model. As those elements which are not necessary for mapping purposes may be disregarded, the mapping process takes less time. The scope might be limited based on specific assessment objectives by referring to only a subset of the reference model elements or even element types.

In this case the scope contains only the selected elements (base practices) of the Governance Model for Trusted Businesses for evaluating Accuracy governance objective within the Monthly Payroll Calculation process:

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Figure 7: Scope selection from the Governance Model for Trusted Businesses

In order to map your business process against the scope that has been set up, i.e. in order to map it against an excerpt of the reference model, you need to assign these elements to each other. You can do this using the assignment page of the Compliance Workbench:

Figure 8: Mapping business process against the scope

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
By rating a lower level governance objective (e.g. related to the IFC.IC.FRI.BP1: Use Matrices to Detail Information Flows base practice), the hierarchical structure of the scope presents automatic evaluation results for also the higher or aggregated levels calculated by the weight of the element within the structure:

![Diagram of BPM-GOSPEL Governance Capability Assessment Case Study Handbook](image)

**Figure 9: Rating a lower level governance objective**

During individual rating of the scoped elements of governance objectives, the description of the relevant assertions can be visualized and also the linked evidence sources can be looked at:

![Diagram of BPM-GOSPEL Governance Capability Assessment Case Study Handbook](image)

**Figure 10: Checking relevant assertions and the linked evidence sources during rating**

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
These links - embedded into the description field by using simple html editor - can point to other pages or views within Stages (like the referred process definitions in Stages) or to external html sources, like reports of used workflow and document management or even transaction processing (e.g. payroll) systems.

By exporting the scopes and mappings between business processes and reference models, external validation tools can be also used for independent evaluation and qualification of the achievement of governance objectives.
3.6 External Validation by Capability Adviser tool

The Capability Adviser tool supports ISO/IEC 15504 conformant process capability assessments - based on recognized models like ISO/IEC 15504-5, Automotive SPICE™, COSO and others - over the Intra-/Internet, creates Profiles, Assessment Reports and integrates Learning Management Systems to distribute already established best practices.

The Capability Adviser works as an SQL database system and all assessment findings, and reports are stored in a central server database. This allows building corporate wide benchmarking and knowledge databases. Also the Capability Adviser supports through virtual team views the early consolidation of results and led to only 2 hour consolidation session per process instance, whereas before this took between 4 to 8 times more effort. In the latest system release Capability Adviser became an information and learning tool for all work places affected by SPICE. Also Capability Adviser is available in different sizes and the smallest portal is affordable even for small companies.

The interface between Stages platform and Capability Adviser tool extends the control over business processes by allowing external assessors/auditors to effectively perform compliance audits (Level 1 assessments) and capability assessments (Level 1-5) for process improvement (consulting) and capability determination (assurance) purposes. While Stages platform provides modelling solution focusing on the business-driven process descriptions and their implementation with useful mappings to elements of the configured generic models, the Capability Adviser tool is more scoping on the assessment work based on the recognized ISO/IEC 15504 conformant process assessment models and using the instances of the business process elements as evidence references.

By using the interface between Stages and Capability Adviser, the following workflow can be followed:

- Business process owners are working on the Stages portal. They are uploading/storing their business process descriptions, control information, mappings to reference models, and the links to the workflow and documentation management and transaction processing systems.

- The Capability Adviser tool is used to perform an assessment on the compliance with reference models and governance capability evidenced by the performed business processes.

- A major part of the assessment work is collecting the evidences. They proof and describe how the company works according to the defined processes. The assessed/audited team usually needs to upload and assign their work products as evidences in the Capability Adviser. To improve the evidence collection phase, the documents and references (links) already implemented and used by Stages are electronically imported as URL links and assigned to the correct process elements into the Capability Adviser.

- Then the assessors are able to directly open the evidences from Stages during the assessment.
Figure 11: Evidence table viewed in Capability Adviser

Once the evidence collection is completed than assessors will

- rate process attributes, so that the participant receives formal capability level and attribute rating profiles;
- make notes to highlight areas where a level of competence has been demonstrated;
- make notes to highlight areas where competence is missing and/or why evidence is not sufficient;
- produce an assessment log including all ratings and comments.

Figure 12: Rating and commenting compliance by Capability Adviser

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
4. Integrated Assurance Management Scenarios supporting Enterprise Governance

4.1 Comments for Implementing Integrated Assurance Management Scenarios

In this case study handbook the application of the Governance Model for Trusted Businesses is presented within a real outsourcing service environment. This sample business environment has internationally standardized (SOC 1 and SOC 2) 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 Integrated Assurance Management scenarios of this case study handbook 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. Normally at a business unit or organization level, the selected governance objectives might be achieved and evidenced through assertions at more business processes, so one business process is typically not providing a baseline for all governance objectives. Furthermore, some of the governance objectives are supported by entity-level control processes, while others by process-level controls or by a combination of these levels. This means, that the “pool” of evidences can be retrieved from different types of information sources, like company’s documentary (filing), transaction processing or work-flow management systems.

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 significantly different scoping approach. The key business processes are viewed as instances of business performance at different operational and organizational levels, so the Integrated Assurance 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 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.

At the Managing Operational Performance scenario, the capability profiles of the baseline business process will show how the management keeps under control of these processes. Normally the Performance Management and Work Product Management process attributes of the Managed (level 2) capability are sufficient to provide reasonable assurance to achieve the performance objectives of the business operation -
like fulfilling service or product specification and delivery time requirements. Targeting higher capability levels for a business process is also reasonable when its performance objectives are directly linked to customer satisfaction, operational effectiveness or even to strategic objectives. For example Monthly Payroll Calculation process related performance metrics (e.g., number of calculations, resource usage, error rates, missed deadlines, etc.) are also applicable indicators of business reliability, operational effectiveness and market recognition within the different time horizons of the specific enterprise goals. The higher process capability of the Monthly Payroll Calculation process means the more extended management and risk treatment practices concerning to the objectives of customer satisfaction, pay-off and order renewal in shorter periods, and of economical sustainability in longer terms. Quantitative measures of key product or service deliveries at recognized quality level are applicable to establish risk tolerance indicators. For example increasing error rates should indicate management actions to improve integrity of the calculation process, technology support and human skills. Unsatisfactory volume (or growth) of monthly transactions should force management to implement changes not only in resource allocation, but also to reorganize business processes and human capacity, or even reconsider business scope, strategy and company structures.

At the Managing Performance Reliability scenario the Satisfaction, Accuracy and Data Protection objectives related governance practices are selected for implementation and improvement in order to enable achievement of pay-off cycle related business objectives, like customer retention and capacity utilization. These practices are also supporting the achievement of Performance Management and Work Product Management process attributes of the Managed (level 2) capability for the baseline business processes. For example Accuracy and Data Protection objectives are helping to identify Work Products related requirements in specific IT-enabled business environments, as of the payroll processing.

The risk appetite at this operational level can be identified as the coverage of business processes by the Satisfaction, Accuracy and Data Protection objectives related governance processes. This means that not all, but the relevant set of the business activities should be covered and there is an interrelation between the capability profiles. The wider coverage of business processes has been achieved, the more reasons appear to investigate capability profiles of the related governance processes. The achievement of the - level 2 - Performance Management and Work Product Management attributes for the business processes will be evidenced by the outcomes of the Satisfaction, Accuracy and Data Protection objectives related governance processes. And vice versa, for example the performance of the “Ensure Systems Security” IT governance/control process (from COBIT) is better evidenced by the coverage of payroll operational processes, than by simple checking the related IT projects or functions. The base practices and work products of the governance processes should be evidenced by the underlying business operation. E.g. avoiding system security incidents has to be proved by the payroll operation. A payroll calculation process at Managed capability level will provide more systematic evidences for the Process Performance attribute of the “Ensure Systems Security” IT control process by setting the relevant performance objectives and work product requirements for payroll calculation.

At the Managing Operational Effectiveness scenario the Exploitability, Process Integrity and Competency objectives related governance practices are selected for implementation and improvement in order to enable achievement of (quarterly or yearly) reporting period specific business objectives, like profitability and agile resource allocation. As these practices provide business unit level framework for effective development and deployment of resources, process control and competency, the achievement of Process Definition and Process Deployment attributes of the Established (level 3) capability profiles for the business processes can be evidenced by them. It is also important to avoid unnecessary or over regulation of business processes: the business unit (or entity) level controls should be implemented not just in compliance with generic control models, but by keeping in mind the business unit level “Usefulness” and “Efficiency” objectives. It is not reasonable to maintain business unit level documentation of those procedures which are not aligned with the business objectives. Documenting, implementing and auditing those procedures which are in conflict either with operational efficiency or simply with process performance objectives, have no value for the organization. Most of those model based compliance works which are not driven by the business unit’s specific objectives are just waste of time and efforts. For example scope of business or quality procedures (manuals) should be determined by keeping the impact on business unit
goals in mind, otherwise management and staff will continuously override these internal rules. Internal rules and guidelines such as for investment or procurement procedures should also have deployment or tailoring guidance allowing customization based on business conditions.

The risk appetite at this organizational level can be identified as the coverage of business processes by the Exploitability, Process Integrity and Competency objectives related governance processes. For example the internal rules and tailoring guidance for managing business unit level resources, quality procedures, process descriptions and human skills are kept by the payroll operational manager in supervising how payroll staff follows them in individual service projects. Therefore the Managed (level 2) capability profiles for the Satisfaction, Accuracy, Data Protection, Exploitability, Process Integrity and Competency objectives related governance/control processes will enable the payroll business processes to achieve Established capability (level 3), when the lower risk level is reasonable for achieving profitability and agile resource allocation targets. The Managed level of the referred governance processes emphasizes the management’s awareness of performance objectives and documentation criteria for implementing business unit (or entity) level operational rules. In smaller organizations or in case of less rule-sensitive services (like reacting to ad hoc advisory requests), there is no need to overregulate all business activities. Performed - level 1 - profiles of the governance processes related to key business activities might be also sufficient, when management considers the higher risk exposure with control cost savings adequately.

Management’s attitude towards control risk taking should be validated by the Managing Operational Risks scenario, where the Risk Awareness and Control Efficiency objectives related governance practices are selected for implementation and improvement. Quantitative Performance Measurement is necessary at each operational and organizational level by considering specific time-horizons of the business objectives. The Predictable - level 4 - profiles of the relevant business processes are enabled by the Managed (level 2) capability profiles for the Satisfaction, Accuracy, Data Protection, Exploitability, Process Integrity, Competency, Risk Awareness and Control Efficiency objectives related governance/control processes. The Predictable process capability ensures that the performance of the business process (e.g. Monthly Payroll Calculation) supports the achievement of the related business goals within tolerable limits. For example, if the reasonable business revenue, cash flow, operating margin and unit cost targets were achievable by performing ca. 10.000 calculations per month with a tolerable limit of 500 less or unpaid, then the Predictable level of operational processes will provide high level of assurance, that in case of the forthcoming customer orders, the business unit will provide the business performance in alignment with the stakeholders’ needs.

Measurable Risk Management performance objectives can be established by the capability targets of the business and governance processes, and by the tolerance levels (control limits around Enterprise Goals) used by the risk treatment cycles. However, the consulting, improvement and assurance efforts and costs might differ e.g. at Managing Operational Performance or at Managing Operational Effectiveness scenarios. Where the risk treatment cycle is more frequent, then the less consulting or assurance cost would gain faster benefit return. For example a simple improvement - like better technology support - in payroll calculation will cause immediate and repeatable benefits. Implementing, assessing and improving processes at Established capability level might take more effort and slower, but potentially higher return on investment. Automating an activity level control within payroll calculation (e.g. evaluating differences from previous calculation results) might have relatively low costs, but immediate benefits of less personal effort, while changing client’s data takeover rules and procedures definitely requests more implementation time and effort with slower return, but will evidently improve data processing integrity, client satisfaction, resource utilization and profitability.

At the Managing Strategic Directions scenario the Competitiveness, Accountability and Commitment objectives related governance practices are selected for implementation and improvement in order to enable achievement of strategic planning period specific business objectives, like revenues and cash flow. As these practices provide the enterprise level framework for setting business strategy and market positioning, management’s accountability and commitment towards internal and external stakeholders, they also support the achievement of Process Definition and Process Deployment attributes of the Established (level 3)
capability profiles for all relevant governance processes. Theoretically above the achieved level 3 profiles the Risk Management practices with applicable Quantitative Performance Measurement - like process capability gaps based risk assessment - would enable the achievement of Predictable (level 4) attributes of governance processes; however this would be reasonable only when measurable links between the capability level of governance processes and the achievement of business goals were evident. As Risk Management and Internal Control systems do not provide absolute assurance for achieving business goals due to their inherent limitations (like management’s bad decisions or override of controls), setting Predictable capability level target for governance processes is generally not reasonable.

In case of public or listed companies, the high level information about Competitiveness, Accountability and Commitment objectives related governance practices are available in company institutional documents, governance reports and other disclosure statements; however their format and content are typically less informative than would be needed by the external stakeholders. Furthermore the prevalent “comply or explain” format of governance reports doesn’t help to understand what is really going on. There are explanations of why criteria are missing, but no information available how and in what extent the “compliant” items work, which is more or less in conflict with the transparency requirements.

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, ESPICE) or generally accepted (e.g. privacy) principles. The full coverage of the governance objectives related processes - by implementing the above mentioned Integrated Assurance Management scenarios - lets organizations 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 - should cover all those business processes and information sources, which provide the sufficient evidences for management assertions concerning to the effective and efficient implementation.

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.
4.2 Managing Operational Performance

4.2.1 Context and Specific Learning Objectives of Managing Operational Performance

The following figure presents role of the Managing Operational Performance scenario in supporting of Enterprise Governance:

![Diagram of Managing Operational Performance](image)

Figure 13: Role of the Managing Operational Performance scenario in Enterprise Governance

In the context of Managing Operational Performance, Enterprise Governance should focus on those issues which are considered as relevant for the following sample management problems:

1. My organization (business unit) provides services or products according to internal or external specifications, however by not keeping delivery deadlines and quality requirements in all cases.
2. Quality issues in product or service delivery request extra effort and/or waste resources.
4. Frequent overwork times cause extra production costs and/or employees’ dissatisfaction
5. Insufficient resources set back of achieving production or service targets.
Normally these issues are occurring and being managed in different time-scale than of the other Integrated Assurance Management scenarios. Managing Operational Performance is limited to the individual instances of the business processes and activities by considering service or product delivery requirements and schedule. Managing Performance Reliability considers contractual pay-off cycles with parallel or reoccurring business operational cycles, while Managing Operational Effectiveness typically has the time-horizon of the budgeting or reporting periods. Managing Strategic Directions is focusing on longer perspectives. Operational Risk Management takes each governance objective into its specific time-horizon when setting risk criteria and measurable risk levels for selecting treatment options and evaluating their effectiveness.

Any reoccurring deviation from performance objectives like rate of performed errorless payroll calculations to planned or scheduled and rate of used capacity to planned (rates per month of payroll processing) will call the management’s attention to check whether Operational Performance objectives are adequately established. Furthermore some operational performance metrics - like more than planned resource usage or frequent corrective actions within operational life-cycles - are going to be early indicators of reliability problems coming to surface only by pay-off with the customer. So solving problems of Operational Performance will limit the potential root causes of Performance Reliability issues.

For detecting root causes of Operational Performance failures we should focus on operational and supporting business processes. As a business operation incorporates processes and activities in order to achieve enterprise goals set for operational and organizational levels (by creating or protecting values of the organization), the target capability levels of these processes have to be established in accordance to these goals. At lower operational level like performing a monthly payroll service based on requirements and schedule agreed with the customer, the adequacy of the performed business operation against specific processing or compliance requirements and against generic performance management criteria should be assessed. To systematically assure the achievement of Operational Performance objectives, the business activities should be formally described according to the process description requirements of ISO/IEC 15504 (by setting relevant purpose statement together with those outcomes which are sufficient and necessary to fulfil process purpose). For these processes the - level 2 - Managed capability requirements of the ISO/IEC 15504 measurement framework are applicable.

Reoccurring deviations from Operational Performance objectives maybe rooted from the capability gaps of performed business processes in scope. Assurance providers should consider whether the operational management supports the employment of ISO/IEC 15504 conformant business processes, and whether the Process Performance, Performance Management and Work Product Management attributes are assessable.

Management actions taken during a reporting period (e.g. covered by quarterly or yearly financial or management statements) to achieve - level 2 - Managed capability for all relevant operational and supporting processes should be monitored by the board or other supervisory bodies (or by equivalent functions of the entity), and adequate level of transparency to all of the stakeholders should be provided by management disclosures.

This part of the case study material is focusing on the Managing Operational Performance scenario, which enables achievement of performance goals such as keeping product or service requirements and schedule and using resources as planned.

The Managed - level 2 - capability of the implemented business processes enables the organization:

- establishing operational plans for the performance of the relevant set of business processes supporting organization’s business operation;
• acting to ensure effective communication regarding the performance of the business processes, through clear assignment of responsibilities and authorities to involved parties;

• allocating adequate resources and information to ensure implementation of the operational plans;

• monitoring performance of the business processes against plans in the individual operational instances;

• taking action to address deviation from planned performance of the business processes;

• identifying compliance requirements for the management of outputs developed or maintained by the processes;

• taking action through appropriate reviews and control mechanisms to ensure that the compliance requirements for output management are satisfied.

The enabling business practices are derived from ISO/IEC 15504 process attributes:

• The Process Performance attribute is a measure of the extent to which the process purpose is achieved.

• The Performance Management attribute is a measure of the extent to which the performance of the process is managed.

• The Work Product Management attribute is a measure of the extent to which the work products produced by the process are appropriately managed.

Applicable measures:

• Performance ("usefulness")
  - Indicator: Performance Rate (e.g. actual errorless calculations/planned calculations)
  - Time-horizon: operating cycles (e.g. a month of payroll processing)

• Expenditure ("efficiency")
  - Indicator: Operating Costs (e.g. hourly rate of payroll)
  - Time-horizon: operating cycles (e.g. a month of payroll processing)

In this part of the case study related to Managing Operational Performance scenario, the Process Performance, Performance Management and Work Product Management attributes are selected to provide applicable use cases for the following learning objectives:

• Which key risk and risk factors are mitigated by the objectives referred by
  – The Process Definition of the operational and supporting processes in context of the business environment and stakeholders’ expectations
  – The Performance Management attribute measuring of the extent to which the performance of the process is managed
  – The Work Product Management attribute measuring of the extent to which the work products produced by the process are appropriately managed
• How to define business processes for assessing **Process Capability** in operational and organizational contexts by achieving - ESPICE SUP.10 - Process Definition outcomes:
  
  o **Standard processes, needed to accomplish business objectives, are established and maintained, including responsibilities, accountability and authority for its management.**
  
  o **Detailed tasks, activities, input/output work products of the standard processes are identified, together with expected performance characteristics.**
  
  o **Allowed modifications and approval mechanisms are established and maintained for the standard processes from which approved processes are tailored and established for projects, programs, services, organizations, or the enterprise.**
  
  o **Goals, performance data, and other assets that support the processes are collected, maintained and communicated.**
  
  o **Process assets (processes, allowed tailoring, approval mechanisms, process objectives, measures of process performance) are collected, maintained, and communicated.**
  
  o **The implemented processes are approved as well-defined derivatives of the standard processes, including support processes, whose purposes and interrelationships are coordinated.**

• How to implement and evaluate generic practices evidencing achievement of **Performance Management** attribute through the following outcomes:
  
  o **objectives for the performance of the process are identified;**
  
  o **performance of the process is planned and monitored;**
  
  o **performance of the process is adjusted to meet plans;**
  
  o **responsibilities and authorities for performing the process are defined, assigned and communicated;**
  
  o **resources and information necessary for performing the process are identified, made available, allocated and used;**
  
  o **interfaces between the involved parties are managed to ensure both effective communication and also clear assignment of responsibility.**

• How to implement and evaluate generic practices evidencing achievement of **Work Product Management** attribute through the following outcomes:
  
  o **requirements for the work products of the process are defined;**
  
  o **requirements for documentation and control of the work products are defined;**
  
  o **work products are appropriately identified, documented, and controlled;**
  
  o **work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.**
4.2.2 Selecting the Scope of the Management Assertions for Managing Operational Performance

A consistent risk assessment should be performed as the first step to establish management assertions by linking business activities to applicable governance practices and capability profiles for supporting the relevant governance objectives.

In case of lower level operational performance objectives, the applicable governance practices are those which help to establish organizational context and assessable format of business activities. This is important because we use business process descriptions derived from the specific organizational and business environment, as they are typically not covered by generic reference models. Therefore the ESPICE SUP.10 Process Definition requirements may be applied as assertion criteria for presenting the specific business operation. By this way the formalized business processes will be assessable against capability level attributes according to the ISO/IEC15504 measurement framework.

By using the definition of risk as “effect of uncertainties on objectives”, during the Managing Operational Performance scenario we have to identify the risk criteria (tolerances and appetite) for governance objectives which are related to the Performance goals. In terms of performance objectives we use the “Usefulness” and “Efficiency” measures for setting metrics in time-horizon of operating cycles (e.g. a month of payroll processing), for example:

- Performance measured by actual performance figures (indicators)
- Expenditures measured by operating costs

For ensuring risk optimisation we need targets and tolerances e.g. measured by:

- Percentage of accepted performance figures compared to planned (e.g. actual errorless calculations/planned calculations) for service cycles and
- Rates of used effort and resources against planned (e.g. payroll staff hours for monthly payroll calculation).

The business operation should have such risk criteria which are applicable to measure effective risk treatment for achieving performance and expenditure related goals by applying enabler practices in achievement of process attributes of the capability level targets. Generally the minimum requirement is achieving fully (over 85%) of the outcomes specified for the assessed business process and largely (over 50%) of the generic outcomes of both the Performance Management and Work Product Management - level 2 - attributes.

When precisely given regulatory or customer (e.g. supply chain management, safety, healthy or ethical) requirements should be kept, then either applicable processes from a proposed/recognized reference model can be adapted as part of the business operation (e.g. industry specific SPICE processes) or these requirements should be set as compulsory outcomes of the defined business processes in scope.

These compliance requirements are normally established by parties during contracting. For example Service Level Agreements may consist of detailed references to applicable processes and capability profiles; however implementation will be highly dependent on both sides, especially when business processes involve roles and activities with shared responsibilities.

For supporting risk assessment the following risk table for the Operational Performance related objectives can be used to understand key risk areas and applicable practices as risk responses:
<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable Requirements</th>
<th>Application Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Losses due to performance failures, such non-compliance to service or</td>
<td>Operational and supporting processes are not established adequately</td>
<td>Operational and supporting processes are established in context of the</td>
<td>Process Definition (ESPICE)</td>
<td>The organization applies practices to identify, define and maintain a standard set of processes and description of allowed tailoring that can be used to establish the processes that are used in execution of business operation.</td>
</tr>
<tr>
<td>product requirements, missed delivery deadlines, wasted efforts and</td>
<td>Operational and supporting processes are not performed in a managed way</td>
<td>process performance is planned, monitored and adjusted during execution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>other resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inputs and outputs are not managed effectively</td>
<td>Work Products are appropriately established, controlled and maintained</td>
<td>Work Product Management (ISO/IEC 15504)</td>
<td></td>
<td>The organization applies generic practices for achieving capability level 2 Work Product Management process attributes.</td>
</tr>
</tbody>
</table>

Table 5: Operational Performance related risk areas

Performance failures have both immediate and longer term effects. Immediate effect is missing the operational targets measured by performance indicators and ineffective usage of resources. The longer term effects are the recurring customer dissatisfaction, the higher than planned operational costs or unpaid overtime works, and even non-compliance penalties or customer claims.

Increasing or recurring performance defaults and unexpected expenditures will lead to losses in business. The implemented governance practices are tools for improving operational performance to minimize potential losses and to increase effectiveness.

The business processes defined in context of organizational goals and in applicable format for ISO/IEC 15504 process assessment provide implementation instances for assessing - level 2 - Managed capability attributes for purpose of process improvement and/or capability determination (assurance) to enable the organization:

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
• establishing operational plans for the performance of the relevant set of business processes supporting organization’s business operation;

• acting to ensure effective communication regarding the performance of the business processes, through clear assignment of responsibilities and authorities to involved parties;

• allocating adequate resources and information to ensure implementation of the operational plans;

• monitoring performance of the business processes against plans in the individual operational instances;

• taking action to address deviation from planned performance of the business processes;

• identifying compliance requirements for the management of outputs developed or maintained by the processes;

• taking action through appropriate reviews and control mechanisms to ensure that the compliance requirements for output management are satisfied.

Of course the higher than level 2 capability targets of the business processes in scope of the business operation might be also reasonable for providing higher assurance, but evidently at higher cost.

The ESPICE SUP.10 - Process Definition outcomes used as assertion criteria make the Governance Capability Assessment methodology applicable for evaluating business processes even against Established (level 3) or higher capability. Without the organizational contexts driven by ESPICE SUP.10 - Process Definition outcomes, only the operational instances (e.g. single or recurring service or product delivery projects) would be assessable.

The set of defined business processes and the target Process Capability Attributes comprise those risk criteria against the business performance should be assessed. Evaluation of Process Attribute Gaps (between target and assessed capability) provides measurement of residual risk status.
4.2.3 Defining Process Outcomes for Managing Operational Performance

The following example shows capability level 2 scoping for the Monthly Payroll Calculation business process presented in chapter 3.4. The process description comprises the purpose statement and relevant outcomes as follows:

**Purpose statement:** The purpose of the Monthly Payroll Calculation process is to perform monthly payroll calculation tasks on behalf of an entity by processing employment data changes, working and absence time information, ad hoc payments or deductions, legal or regulatory changes and other relevant information as inputs for preparing outputs according to the regulatory and contractual requirements concerning their content, format, delivery methods and deadlines with expected professional diligence.

**Outcomes** as defined by activity goals:

1. Setting up and preparing for the payroll cycle
2. Collecting and recording clients' monthly payroll information based on agreed data-handling rules
3. Input data control and processing for payroll calculation with Client's control
4. Checks and verifications of payroll calculation processing information
5. Submission of all monthly payroll calculation outputs based on regulatory and agreed client's requirements
6. Regulatory monthly reporting and documenting monthly payroll calculation process

The process activities relevant for these outcomes together with their input and output work products - as presented in chapter 3.4 - are used as process performance - level 1 - indicators.

"Assessors will try to verify that the people performing the process understand the purpose of the process itself and perform the necessary actions. The work products resulting from performing the activities, together with input work products, are further evidence of process performance. However, the simple existence of these work products is not sufficient; it should be evident that they contribute to achieving the process purpose." (ISO/IEC 15504-3:2004)

For careful consideration of process performance related risk criteria, management should set and present metrics like described in the following sample table. Where current metrics show significant deviation from management’s expectations (risk appetite), the related activities (maybe also in other processes) should be redesigned and improved. Where current metrics are available and satisfactory to reasonable risk appetite, the process activities are applicable as process performance indicators for rating achievement of Process Performance (level 1) attribute.

Next table shows sample metrics related to the outcomes of the Monthly Payroll Calculation process:
<table>
<thead>
<tr>
<th>Outcomes of the Monthly Payroll Calculation process</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up new payroll cycle</td>
<td>Coverage of volume and requirement changes per service elements (e.g. only 70% of changes were identical during preparation)</td>
<td>Coverage of approved changes in capacity allocation for infrastructure, skills, material and human resources (e.g. only 80% of necessary changes in capacity allocation is admitted by the client)</td>
</tr>
<tr>
<td>Collecting and recording clients' monthly payroll information based on agreed data-handling rules</td>
<td>Rate of exceptional cases per information types (e.g. 10% of employment data changes with missing formatting rules)</td>
<td>Rate of overtime due to exceptional data takeover per staff category (e.g. 20% extra effort for manual data input by payroll clerk)</td>
</tr>
<tr>
<td>Input data control for regulatory compliance, completeness and consistency, processing input data for payroll calculation</td>
<td>Rate of non-processed data per input types (e.g. 20% timesheet data found inconsistent)</td>
<td>Rate of overtime due to managing data errors per staff category (e.g. 20% extra effort for manual document checks and discussion by payroll clerk)</td>
</tr>
<tr>
<td>Checks and verifications of payroll calculation processing information</td>
<td>Coverage of requirements (check-list) per service elements (e.g. exceptional cases are double checked)</td>
<td>Rate of actual to planned (allocated) verification effort (e.g. 100% extra verification effort due to exceptional cases)</td>
</tr>
<tr>
<td>Submission of all monthly payroll calculation outputs based on regulatory and agreed client's requirements</td>
<td>Rate of approval per service elements (e.g. accounting report rejected due to formatting error)</td>
<td>Rate of extra output submission efforts and resources (e.g. 10% extra work due to manual report formatting)</td>
</tr>
<tr>
<td>Regulatory reporting and documenting monthly payroll calculation process</td>
<td>Performance rates of reporting/documentation elements (e.g. acceptance by tax authorities)</td>
<td>Rate of extra reporting or documenting works (e.g. 10% more efforts for document filing)</td>
</tr>
</tbody>
</table>

Table 6: Outcomes of Monthly Payroll Calculation process with sample metrics
The sample scope setting is targeting - level 2 - Managed capability by fully (more than 85%) achievement of Process Performance (level 1) attribute, and largely (over 50%) achievement of Performance Management and Work Product Management (level 2) attributes according to ISO/IEC 15504 (SPICE) measurement framework. Achievement is measured by using a four point ordinal scale.

![Four point ordinal scale for evaluating the achievement of process attribute](image)

**Figure 14: Four point ordinal scale for evaluating the achievement of process attribute**

According to ISO/IEC 15504, each process attribute must be rated on a scale from “Not” achieved through “Fully” achieved as follows:

- Not (little or no evidence of the attribute in the process)
- Partially (some evidence of the attribute in the process, though some aspects may be unpredictable)
- Largely (significant evidence of the attribute in the process, though some variation may exist)
- Fully (the attribute is completely and consistently found in the process with no significant weakness in process performance detected)

Using such a scale, the difference between “Partially” and “Largely” is significant since, to achieve a given level, all attributes at that level must be “Fully” or “Largely” achieved (with all attributes at lower levels “Fully” achieved). One goal of the scale was to avoid an “average” rating, either disguising the need for or creating an arbitrary need for improvement.
4.2.4 Applying generic - level 2 - Managed capability indicators as risk criteria for Performance Goals

Managed (level 2) process capability requests that (above of “Fully” achievement of the Process Performance attribute) the Performance Management and Work Product Management attributes are minimum largely achieved (while Process Performance attribute is fully achieved). The following generic outcomes should be evidenced for the selected business processes in scope of the business operation (e.g. Monthly Payroll Calculation):

- for Performance Management attribute:
  - Objectives for the performance of the process are identified;
  - Performance of the process is planned and monitored;
  - Performance of the process is adjusted to meet plans;
  - Responsibilities and authorities for performing the process are defined, assigned and communicated;
  - Resources and information necessary for performing the process are identified, made available, allocated and used;
  - Interfaces between the involved parties are managed to ensure both effective communication and also clear assignment of responsibility.

- for Work Product Management attribute:
  - Requirements for the work products of the process are defined;
  - Requirements for documentation and control of the work products are defined;
  - Work products are appropriately identified, documented, and controlled;
  - Work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.

The above requirements are generic to all governance and business processes in scope. The mapping between Managed process capability (level 2) generic outcomes and enabling governance practices provides additional insight to the enterprise governance framework. The level 2 outcomes of managing process performance are aimed by the Project and Quality Management related practices of the Exploitable Operation governance process as shown in the next table. However this process is defined as an enabler of the Managing Operational Effectiveness - a business unit level - scenario. This observation is evidently reasonable, as the Managed capability level of a business or a governance process indicates that business unit management is committed to use the applicable governance practices - supporting business operation - in alignment with business unit level goals, such as profitability and agile resource allocation.
<table>
<thead>
<tr>
<th>Generic Outcomes of Managed (level 2) Capability</th>
<th>Enabling Governance Practices of Project and Quality Management</th>
</tr>
</thead>
</table>
| Objectives for the performance of the process are identified | **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. |
| Performance of the process is planned and monitored | **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 maintain a complete set of plans for providing the products and services throughout the project life cycle.  
**GVM.8.BP19**: Monitor Project Performance. Monitor and track project activities and results against plans and baseline.  
**GVM.8.BP22**: Close Project. Close the project formally using appropriate organizational mechanisms and update organizational process assets. |
| Performance of the process is adjusted to meet plans | **GVM.8.BP16**: Direct and Manage Project Execution. Perform the work defined in the project plan to achieve the project’s objectives.  
**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 |
### Generic Outcomes of Managed (level 2) Capability

<table>
<thead>
<tr>
<th>Enabling Governance Practices of Project and Quality Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>problems.</td>
</tr>
</tbody>
</table>

**Responsibilities and authorities for performing the process**
are defined, assigned and communicated

- **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.

**Resources and information necessary for performing the process** are identified, made available, allocated and used

- **GVM.8.BP5: Estimate Project Resource Requirements.** Estimate the project effort, cost, schedule and other resource requirements.
- **GVM.8.BP12: Plan Procurements.** Plan and document project purchasing decisions.
- **GVM.8.BP17: Distribute Information.** Make relevant or established information available to project stakeholders as planned.

**Interfaces between the involved parties** are managed to ensure both effective communication and also clear assignment of responsibility

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

**Requirements for the work products of the process** are defined

- **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.

**Requirements for documentation and control of the work products** are defined

- **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.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.

**Work products are appropriately identified, documented, and controlled**

- **GVM.8.BP3: Monitor Product and Service Quality.** Objectively compare, measure and evaluate work products and services against the requirements and standards that define them.
- **GVM.8.BP4: Monitor Noncompliance Issues.** Monitor and track...
### Table 7: Mapping Managed Process Capability with enabling Governance Practices

<table>
<thead>
<tr>
<th>Generic Outcomes of Managed (level 2) Capability</th>
<th>Enabling Governance Practices of Project and Quality Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>adjusted as necessary to meet requirements</td>
<td>noncompliance issues and support their resolution via escalation to senior management if necessary.</td>
</tr>
<tr>
<td></td>
<td><strong>SUP.3.BP8: Monitor and Evaluate the Effect of Changes.</strong> Monitor the status of quality improvements on products and services and evaluate the effect of changes after they have been implemented.</td>
</tr>
</tbody>
</table>

As “Usefulness” and “Efficiency” are not interpretable within the process capability dimension, there is no meaning to establish such metrics for generic practices of level 2 - or higher - Process Attributes. These metrics are applicable in business context of the processes by providing tool for defining and/or adapting economically meaningful process performance indicators.
4.3 Managing Performance Reliability

4.3.1 Context and Specific Learning Objectives of Managing Performance Reliability

The following figure presents role of the Managing Performance Reliability scenario in supporting of Enterprise Governance:

![Managing Performance Reliability Diagram]

Figure 15: Role of the Managing Performance Reliability scenario in Enterprise Governance

In the context of Managing Performance Reliability, Enterprise Governance should focus on those issues which are considered as relevant for the following sample management problems:

1. My organization (business unit) provides services or products according to internal or external specifications by keeping delivery deadlines and quality requirements, however my customer is not fully satisfied, there are complaints or indemnity claims during discussions for acceptance or even refusal of invoices.

2. My customer is ready to approve delivery of services or products if only additional performance is provided referring to changes of external conditions (e.g. additional work to satisfy new regulatory requirements not considered during contracting).

3. My customer is satisfied and happy, but service or product delivery takes significantly more overall capacity from my organization than planned during resource allocation.

4. Customer requests extensive changes of documentation over product or service delivery which might be incompatible with my organization’s information system or capacity (e.g. changing to new specific formatting or reporting requirements after contracting).
5. Customer needs additional assurance over integrity, security, confidentiality and privacy of client’s information used, processed and stored during or after service and product delivery (e.g. availability and cooperation during regulatory audits or control assessments within or after contracting period).

Normally these issues are occurring and being managed in different time-scale than of the other Integrated Assurance Management scenarios. Managing Operational Performance is limited to the individual instances of the business processes and activities by considering service or product delivery requirements and schedule. Managing Performance Reliability considers contractual pay-off cycles with parallel or reoccurring business operational cycles, while Managing Operational Effectiveness typically has the time-horizon of the budgeting or reporting periods. Managing Strategic Directions is focusing on longer perspectives. Operational Risk Management takes each governance objective into its specific time-horizon when setting risk criteria and measurable risk levels for selecting treatment options and evaluating their effectiveness.

Any reoccurring deviation from reliability objectives like customer retention and capacity utilization (rates per pay-off cycles) will call the management’s attention to check whether lower level Operational Performance objectives are adequately fulfilled as operational performance failures might also cause customer dissatisfaction. Furthermore some operational performance metrics - like more than planned resource usage or frequent corrective actions within operational life-cycles - are going to be early indicators of reliability problems. Most of the reliability issues are coming to surface only by pay-off with the customer, so early indicators from Operational Performance will help management to be more prepared.

In case of no root cause having been found at Managing Operational Performance, then Satisfaction, Accuracy and Data Protection objectives and related governance practices should be assessed whether the selection of practices and their capability targets are aligned with the Reliability Goals or the implemented practices are achieving their target capability levels.

Reoccurring deviations from customer retention and capacity utilization objectives are early indicators of those Operational Effectiveness issues which might be identical only by closures of budgeting or reporting periods. Assessment and improvement of Satisfaction, Accuracy and Data Protection objectives related process capability profiles are necessary risk management actions not just enabling overall customer satisfaction but also driving to better Operational Effectiveness.

Management actions taken during a reporting period (e.g. covered by quarterly or yearly financial or management statements) to achieve Satisfaction, Accuracy and Data Protection objectives - together with the other governance objectives - should be monitored by the board or other supervisory bodies (or by equivalent functions of the entity), and adequate level of transparency to all of the stakeholders should be provided by management disclosures.

This part of the case study material is focusing on the Managing Performance Reliability scenario, which enables achievement of Reliability Goals such as satisfaction and trust of users/customers over operational performance.

By the support of this Integrated Assurance Management scenario, the organization:

- ensures user/customer satisfaction based on agreed levels of business operation;
- ensures the accuracy and consistency in data architecture and disclosure elements relevant for business operation, and for supporting data processing integrity;
- is committed to security, confidentiality and privacy principles to avoid unauthorized access to and misuse of confidential data effected by business operation.
The enabling governance processes are:

- Satisfactory Operation, adapting practices from Enterprise SPICE
- Information Reliability, adapting practices from COBIT and COSO
- Data Protection, adapting practices from COSO, COBIT and GAPP

Applicable measures:

- Customer Retention ("usefulness")
  - Indicator: Order Renewals
  - Time-horizon: contracting/pay-off periods

- Capacity Utilization ("efficiency")
  - Indicator: Capacity Utilization Rate
  - Time-horizon: contracting/pay-off periods

In this part of the case study related to Managing Performance Reliability scenario, the Satisfaction, Accuracy and Data Protection governance objectives are selected to provide applicable use cases for the following learning objectives:

- Which key risk and risk factors are mitigated by the governance objectives referred by
  - The Satisfactory Operation application area aiming to ensure customer satisfaction based on agreed levels of business operation.
  - The Information Reliability (Accuracy) application area aiming 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.
  - The Data Protection application area aiming 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.

- How to implement and evaluate application practices evidencing achievement of Satisfaction governance objective through the following outcomes:
  - Requirements are established and maintained based on customer needs and expectations.
  - Business relationship management is effective.
  - Business operation supports its customers by achievement of agreed service level requirements.

- How to implement and evaluate application practices evidencing achievement of Accuracy governance objective through the following outcomes:
  - Effective information architecture and data model are maintained.
  - Information is systematically collected and assessed to detect compliance issues, privacy problems and fraud.
o Control information for automated process settings, data manipulations and calculations are maintained systematically.

- How to implement and evaluate application practices evidencing achievement of Data Protection governance objective through the following outcomes:
  o Preventive controls are maintained to avoid system security incidents.
  o Anti-fraud management program is maintained.
  o Privacy requirements are kept.
4.3.2 Selecting the Scope of the Management Assertions for Managing Performance
Reliability

A consistent risk assessment should be performed as the first step to establish management assertions by linking business activities to applicable governance practices and capability profiles for supporting the relevant governance objectives.

By using the definition of risk as “effect of uncertainties on objectives”, during the Managing Reliable Operation scenario we have to identify the risk criteria (tolerances and appetite) for governance objectives which are related to the Reliability Goals. In terms of reliability we use the “Usefulness” and “Efficiency” measures for setting metrics in time-horizon of contracting payoff periods, for example:

- Customer retention measured by order renewal
- Capacity utilization measured by resource utilization rate

For ensuring risk optimisation we need targets and tolerances e.g. measured by:

- Percentage of successful order renewals for service periods and
- Utilization rates for engaged human resources and infrastructure.

The reliable business operation related Satisfaction, Accuracy and Data Protection governance objectives should have such risk criteria which are applicable to measure effective risk treatment for achieving customer retention and capacity utilization goals by applying governance practices. Applicable governance practices should be selected and implemented by considering their relevance to the above “Usefulness” and “Efficiency” measures.

If a lower level governance practice offered by the Governance Model has no significant relevance for the established Reliability Goals, then there will be no need to apply that. If management specifies a governance practice as relevant for managing reliable business operation within the context of stakeholders’ needs, then the target capability profile for implementing the governance process will include it and will be used as risk criteria (risk appetite). Capability level target should be set aligned with the relevant Enterprise Goals, as in this case in accordance with Reliability Goals.

When the stakeholders’ expectations for Service Organization’s Control (SOC) determining high level Accuracy and Data Protection requirements, the capability profiles of Information Reliability and Data Protection processes shall be set by the optimal (meaningful) coverage of offered governance practices, together with a capability profile aiming higher (e.g. Level 2 - Managed or Level 3 - Established) requirements. The management assertions, monitoring and assurance reports should present how these criteria are kept by managing operational activities and processes. For a small service organization these criteria might be exaggerated, but failure of attestation would cause leaving of major clients. However exaggerated application of governance practices could also cause worse utilization of resources. That is why selecting applicable governance practices and targeting capability profiles of their implementing processes need mature risk management performed by organizational governance.

Satisfactory Service requirements are normally established by parties during contracting. Service Level Agreements may consist of detailed references to applicable governance practices and capability profiles; however implementation will be highly dependent on both sides, especially when business processes involve roles and activities with shared responsibilities.

For supporting risk assessment the following risk tables for the Satisfaction, Accuracy and Data Protection objectives can be used to understand key risk areas and applicable practices as risk responses:

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable Enterprise SPICE processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Losses due to customer dissatisfaction</td>
<td>Requirements are not established adequately</td>
<td>Requirements are established based on customer needs</td>
<td>Requirements (ESPICE)</td>
</tr>
<tr>
<td></td>
<td>Ineffective business relationship management</td>
<td>Business relationship management is maintained</td>
<td>Business Relationship Management (ESPICE)</td>
</tr>
<tr>
<td></td>
<td>Product or service delivery default</td>
<td>Monitoring based on agreed service levels</td>
<td>Operation and Support (ESPICE)</td>
</tr>
</tbody>
</table>

Table 8: Satisfaction related risk areas

Customer dissatisfaction has both immediate and longer term effects. Immediate effect is the worse resource utilization (unpaid service or overwork). The longer term effects of leaving clients and less income are also predictable in repeating failure cases.

Decreasing number of order renewal and lower resource utilization rate per customer will lead to losses in business. The implemented governance practices are tools for improving customer satisfaction to minimize potential losses and to increase possibilities of order renewals or new contracts. The selected governance practices provide implementation instances of the **Satisfactory Operation** governance process enabling the achievement of the following outcomes:

- Requirements are established and maintained based on user/customer needs and expectations.
- Business relationship management is effective.
- Business operation supports its user entities by achievement of agreed service level requirements.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Table 9: Accuracy related risk areas

Reliable information is the precondition of data processing and reporting. Furthermore collecting of control information is also needed for ensuring quality of data processing. Unreliable information will cause extra processing and time and resources followed by manual controls and corrections. Agreed input data architecture and output formats are necessary elements of ensuring customer satisfaction in IT-enabled service environment. The service providers always remain responsible for the errors detected in service outputs by customers or authorities, so data, processing and reporting inconsistencies have to be avoided as much as possible, otherwise extra manual work will be needed. As deadlines and service fees are normally calculated by presuming effective data processing, the accuracy problems have negative effects on customer retention and resource utilization.

Frequent output errors or missed deadlines lead to extra indemnity or compensation costs and general customer dissatisfaction. The implemented governance practices are tools for minimizing manual processing and controls to ensure effective and reliable data processing. The selected governance practices provide implementation instances of the Information Reliability governance process enabling the achievement of the following outcomes:

- Effective information architecture and data model are maintained.
- Information is systematically collected and assessed to detect compliance issues, privacy problems and fraud.

- Control information for automated process settings, data manipulations and calculations are maintained systematically.

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable COSO&amp;COBIT processes and GAPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access to and misuse of confidential data</td>
<td>System security and confidentiality failures</td>
<td>Preventive controls maintained to avoid system security incidents</td>
<td>Ensure Systems Security (COBIT)</td>
</tr>
<tr>
<td></td>
<td>Unauthorized access to and misuse of confidential data</td>
<td>Anti-fraud management program maintained</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Breaching privacy requirements</td>
<td>Active policies and procedures are in place to ensure privacy requirements</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Generally Accepted Privacy Principles (AICPA/CICA)</td>
<td>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).</td>
</tr>
</tbody>
</table>

Table 10: Data Protection related risk areas

Ensuring information security for confidential and privacy data is a strict regulatory and customer requirement especially in outsourcing business environment. Any serious breach might cause indemnity or immediate contract notice. Furthermore this type of dissatisfaction has the biggest damage on reputation of the service provider affecting other contracts as well. In case of using web-based or e-commerce systems, adequate management of data protection issues is even more critical to satisfactory business operation.

The implemented governance practices are tools for minimizing unauthorized access to and misuse of confidential service data. The selected governance practices provide implementation instances of the **Data Protection** governance process enabling the achievement of the following outcomes:

- Preventive controls are maintained to avoid system security incidents.

- Anti-fraud management program is maintained.
• Privacy requirements are kept.

The set of applied governance practices and the target Process Capability Attributes comprise those risk criteria against the business performance should be assessed. Evaluation of Process Attribute Gaps (between target and assessed capability) provides measurement of residual risk status.
4.3.3 Applying Management Assertions for Managing Performance Reliability

Management assertions are setting links between the business processes (and activities) and the governance objective-driven processes (and base practices) offered by recognized reference models (like COSO, COBIT and Enterprise SPICE). Management should reflect to their own business goals and business environment’s expectations by setting target capability profiles for the customized governance objectives (risk appetite) and adequate quantitative control limits of tolerable deviations from Enterprise Goals (risk tolerance). Governance Capability Assessment (Governance SPICE) methodology provides measurement framework for targeting and assessing effectiveness of governance processes (defined by ISO/IEC 15504 compliant reference models) in achievement of governance objectives, however it should be carefully considered at the assessment scope definition, that a governance process might be implemented and applied by more than one business processes (and their instances) within a business operational unit.

For example in the case of Accuracy objective concerning to the Monthly Payroll Calculation business process, the management should determine the management and control activities necessary and sufficient to limit the negative consequences of the inherent business risk related to inconsistency in payroll processing data architecture and disclosure elements.

Theoretically the management should apply a measure for determining direct impact on specific business goals, however at business process level this measure can’t derived directly from “natural” business measures like income, profitability, stock listing rate, market-share, etc. This problem could be resolved by targeting application of governance practices by the business process activities. The more relevant governance practices are applied; the negative consequences are the more likely minimized.

However the adequate structure of performance measurement helps to navigate over applicable governance practices (see Figure 4: Linking Governance Objectives to Enterprise Goals & Measures). The governance practices are enabling achievement of Enterprise Goals, so measurement related to achievement of governance objectives should support in-time status information regarding overall business performance. Furthermore the lower level operational or organizational goals and metrics should be established as enabling indicators for the above governance level.

By this way the appearing deficiencies to target measures of Managing Operation Performance - e.g. delays, errors, overworks in a monthly payroll calculation cycle - might be early indicators of possible failures at Managing Performance Reliability level - e.g. client complains and claims or capacity utilization issues by closing contractual settlement periods. Similarly the metrics indicating deviation from Reliability Goals call the attention for possible consequences in achievement of Organizational Goals at Managing Operational Effectiveness level - e.g. decreasing profitability of the payroll business unit in business reporting period.

For selecting and prioritizing governance practices offered by the reference models, the Managing Performance Reliability scenario offers “Usefulness” and “Efficiency” aspects of business performance. In case of Monthly Payroll Calculation business process, the performance reliability should enable customer retention (measured by order renewal per contracting payoff periods) and capacity utilization (measured by infrastructure and human resource utilization rates).

These two types of metrics help to identify relevance and weight of applicable governance practices in supporting performance objectives. If lack or failure of a governance practice - by considering together with other existing governance practices - represents undesirable uncertainty on keeping “Usefulness” or “Efficiency” goals, then implementation or improvement of the practice will be an adequate risk treatment option. If the lack or failure of
a governance practice has no significant effect on Enterprise Goals - by considering together with other existing governance practices – this practice will be out of the scope of implementation and assurance. Performance measurement is needed to establish the concerning risk criteria and tolerance levels triggering immediate or scheduled management actions.

For example: a failure (performance gap) of COBIT 4.1 PO2.4 Managing Data Integrity practices for Accuracy governance objective in a payroll outsourcing service - using automated data processing - causes undesirable uncertainty in achievement of performance reliability. “Unusual” calculation errors or overtime works already detected during a payroll processing cycle (e.g. monthly calculation) might indicate potential danger of serious client claims or unpaid resource consumption (more than planned capacity usage) during next invoicing also effecting overall satisfaction (future client retention) and service capacity utilization. Client dissatisfaction or capacity utilization problems are early indicators of effectiveness problems at Payroll Service Unit level. In this case an identified performance gap at Managing Data Integrity practice triggers the management actions for process improvement related to the Accuracy governance objective. Even if the payroll data processing is supported by external IT solution (e.g. payroll software), the relevance and importance of Managing Data Integrity will remain within the service provider’s responsibility, however usage of well-reputed or certified IT product or service will simplify the implementation of this governance practice.

For protecting own market position even smaller service providers use in-house IT solutions by considering cost and effort of implementing governance practices against benefit for better performance reliability of business operation.

The lower level metrics like error rate and human overtime work per calculation cycle should be assessed against company targets (or other reasonable benchmark) and measures over pre-established tolerances should trigger the (re)assessment of Managing Data Integrity governance practices. If the assessed performance gap is significant as effecting customer retention or capacity utilization by exceeding their tolerances, then improvement action should be planned and implemented by the management. If detected performance gaps were not affecting significantly the Reliability Goals of payroll outsourcing service, then either the triggering tolerances of lower level performance metrics might be reset, or - more likely - other related governance practices should be also assessed. Relevance and weight of a governance practice should be considered not just as an enabler of the related governance objective (e.g. Managing Data Integrity enables achievement of Reliability Goals), but also as whether its implementation would have effect on the next level Enterprise Goals. E.g. Managing Data Integrity shouldn’t cost more than reasonable in context of Organizational Goals at Managing Operational Effectiveness level (might be measured by operating margin and unit cost).

At corporate level the governance objectives related set of practices comprising ISO/IEC 15504 compliant governance processes - as defined by the Governance Model - are applicable for targeting and assessing them for even higher (e.g. level 2 or above) governance capability. However from the selected business process view, as in the case of Monthly Payroll Calculation, the assessment target is mostly limited to Compliance (1 - Performed) level, as this is the level where the application of specific process outcomes and practices are investigated.

Targeting the Managed (level 2) or even higher level for the governance processes is applicable in the case when capability target of the Managing Performance Reliability scenario were pre-established accordingly (e.g. in compliance with strict regulatory requirements). The higher capability request for Managing Performance Reliability should be determined by the Operational Risk Management function and also takes other effected business processes (e.g. not just the Monthly Payroll Calculation) into the same capability level context.
4.3.4 Selecting specific application practices as risk criteria for Reliability Goals

For fully achieving Process Performance attribute, the following specific outcomes should be evidenced concerning to the governance processes supporting Performance Reliability (of Monthly Payroll Service):

- **for Satisfactory Operation** governance process:
  - Requirements are established and maintained based on customer needs and expectations.
  - Business relationship management is effective.
  - Business operation supports its customers by achievement of agreed service level requirements.

- **for Information Reliability** governance process:
  - Effective information architecture and data model are maintained.
  - Information is systematically collected and assessed to detect compliance issues, privacy problems and fraud.
  - Control information for automated process settings, data manipulations and calculations are maintained systematically.

- **for Data Protection** governance process:
  - Preventive controls are maintained to avoid system security incidents.
  - Anti-fraud management program is maintained.
  - Privacy requirements are kept.

The applied Governance Model for Trusted Businesses offers recognized best practices supporting these outcomes, however not all of them are necessary in context of the specific Enterprise Goals of the organization. Management should select only those practices as assertions, which have evidential link to “Usefulness” and “Efficiency” goals at this operational level. For Managing Performance Reliability of Monthly Payroll Calculation these goals are: reasonable client retention and effective capacity utilization.

For careful consideration, management should set metrics like described in the following sample table. Where current metrics show significant deviation from management’s expectations (risk appetite), the related practice should be implemented or improved. Where current metrics are available and satisfactory to reasonable risk appetite, the application practice can be set for management assertion.

Next table shows sample metrics for application practices supporting Satisfaction governance objective:
### Application Practices for Satisfaction Governance Objective

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usefulness related metrics</strong></td>
</tr>
<tr>
<td>Coverage of service elements by approved requirement specification (e.g. only 80% of service elements have approved requirement specification)</td>
</tr>
<tr>
<td><strong>Efficiency related metrics</strong></td>
</tr>
<tr>
<td>Coverage of approved capacity allocation for infrastructure, skills, material and human resources (e.g. only 75% of necessary capacity allocation is admitted by the client)</td>
</tr>
</tbody>
</table>

**LFC.2.BP1: Identify Requirements.** Identify all types of requirements applicable to customer needs and expectations.

- Ratio of non-standard requirements (e.g. 40% of requirements are related to ad hoc requests)
- Ratio of flexible capacity allocation (e.g. ad hoc effort hours)

**LFC.2.BP2: Derive Requirements.** Derive requirements that may be identified as necessary implications of the identified requirements.

- Ratio of derived requirements (e.g. 40% of requirements are related to client specific reporting formats)
- Ratio of derived capacity allocation for the contracting period (e.g. supporting IT capacity for specific client needs)

**LFC.2.BP3: Analyze Requirements.** Analyze requirements to ensure that they satisfy established quality criteria, including unambiguity, completeness, traceability, feasibility, and verifiability.

- Ratio of analysed requirements (e.g. only 30% of requirements have pre-established criteria)
- Ratio of analysed capacity allocation (e.g. 25% of resources allocated without analysis)

**LFC.2.BP4: Baseline Requirements.** Record, approve, baseline, and place under change control all requirements.

- Ratio of requirements under change control (e.g. 80% of requirements are not followed systematically)
- Ratio of non-controlled changes in capacity allocation requirements (e.g. 40% of changes in resource allocation are not followed)

**LFC.2.BP5: Analyze Requirements Risks.** Document and analyze risks associated with the requirements.

- Frequency of formal risk assessment of requirements (e.g. no documented risk assessment for the requirements)
- Coverage of capacity requirements by formal risk assessment (e.g. only infrastructure capacity requirements are considered)

**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.

- Ratio of analysed and approved requirement changes (e.g. 80% of requirement changes are not approved formally)
- Ratio of approved changes in capacity allocation requirements (e.g. 40% of changes in internal control resource allocation are not approved formally)

**LFC.2.BP7: Ensure and Maintain Requirements Traceability across the Life**

- Coverage of traceability during
- Coverage of capacity allocation traceability

---

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
**Application Practices for Satisfaction Governance Objective**

**Usefulness related metrics**

**Efficiency related metrics**

<table>
<thead>
<tr>
<th><strong>Cycle.</strong> Maintain traceability among requirements and between requirements and plans, work products, and activities initiating corrective action if inconsistencies are identified.</th>
<th>operation (30% of requirements are not identical during operation)</th>
<th>during operation (e.g. only human capacity allocation requirements are traceable)</th>
</tr>
</thead>
</table>

**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.

<table>
<thead>
<tr>
<th>Coverage of relationship types (e.g. contracting, marketing, operational supervision and day-to-day contact levels)</th>
<th>Allocated time and resources per relationship types (e.g. meeting frequency and durations for each contact level)</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Number and types of contacts (e.g. 1-1 dedicated contacts for each level)</th>
<th>Availability of contact types (e.g. during and over business hours for each type)</th>
</tr>
</thead>
</table>

**GVM.5.BP2: 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.

<table>
<thead>
<tr>
<th>Number of dedicated contact positions (e.g. one dedicated person for regular customer satisfaction surveys)</th>
<th>Allocated resources for contact positions (e.g. 1 hour per month for discussing satisfaction survey results with customer)</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Number of relationship attributes (e.g. position, skills, communication language, formality, etc.)</th>
<th>Coverage of relationship attributes by allocated resources (e.g. English speaking in communication of day-to-day operation)</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>Number of value creation opportunities per contracting period (e.g. providing regular newsletter and consultancy on regulatory obligations or changes, new product or service features, etc.)</th>
<th>Allocated resources for communicating value creation opportunities (e.g. number of working hours per pay-off period for advising client)</th>
</tr>
</thead>
</table>

**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.

<table>
<thead>
<tr>
<th>Number and ratio of managed complaints and compliments (e.g. only 4 from 5 complaints of the pay-off period are managed)</th>
<th>Allocated resources for managing complaints and compliments (e.g. operational line manager spends 1 hour per pay-off period to review complaints and</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Practices for Satisfaction Governance Objective</td>
<td>Usefulness related metrics</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>GVM.5.BP6: Create Service Level Agreements. Create Service Level Agreements between the business owner and the product/service supplier.</td>
<td>Coverage of service elements (e.g. SLA might not cover ad hoc consultancy on regulatory changes)</td>
</tr>
<tr>
<td>GVM.5.BP7: Establish a Service Catalog. Establish and maintain a service catalog for communicating with the business.</td>
<td>Ratio of standard service elements (e.g. 90% of service elements are standardized)</td>
</tr>
<tr>
<td>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.</td>
<td>Satisfaction rate per pay-off period (e.g. 100% coverage of agreed service level in monthly payroll calculation)</td>
</tr>
<tr>
<td>LFC.8.BP1: Operate the Product or Service. Operate the product or service in its intended environment according to agreed service levels.</td>
<td>Operational outcome metrics (e.g. number of payroll calculation per month)</td>
</tr>
<tr>
<td>LFC.8.BP2: Establish Methods. Establish methods for monitoring and sustaining required product or service levels.</td>
<td>Coverage of service elements (e.g. non standardized service elements are not covered)</td>
</tr>
<tr>
<td>LFC.8.BP3: Monitor and Evaluate Capacity, Service, and Performance. Monitor and evaluate capacity, service, and performance of the product or service.</td>
<td>Frequency of evaluation (e.g. only once per pay-off period)</td>
</tr>
<tr>
<td>LFC.8.BP4: Confirm Availability of Resources. Confirm availability of required resources (e.g., personnel, parts) to ensure service levels can be sustained.</td>
<td>Coverage of service elements (e.g. only for standard service elements)</td>
</tr>
<tr>
<td>LFC.8.BP5: Perform Corrective and/or Preventive Maintenance. Perform corrective replacement of the product or service</td>
<td>Number of replacing product or service</td>
</tr>
</tbody>
</table>
### Application Practices for Satisfaction Governance Objective

<table>
<thead>
<tr>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>and/or preventive maintenance by replacing or servicing product or service elements prior to failure.</td>
<td>elements prior to failure (e.g. repeated processing outputs)</td>
</tr>
<tr>
<td>LFC.8.BP6: Analyze Failures. Perform failure identification and analysis activities when problems or interruptions occur in the product or delivered service.</td>
<td>additional processing time and working hours for repeating calculation process</td>
</tr>
<tr>
<td>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.</td>
<td>Failure root detection rate per service elements (e.g. 99% for data processing errors)</td>
</tr>
<tr>
<td>LFC.8.BP8: Provide Customer Support. Answer customer and user questions and help resolve problems they encounter.</td>
<td>Effort and resource usage (e.g. 10 working hours for detecting new hardware or software incompatibility problems).</td>
</tr>
</tbody>
</table>

| Number of corrective actions per service elements during pay-off period (e.g. 1 software update due to regulatory changes) | Resource used for corrective actions during pay-off period (e.g. working time for software maintenance and deployment) |
| Ratio of answered questions and resolved problems (e.g. 100% of questions have been answered, 10% problems have remained unsolved during pay-off period) | Resource used to provide customer support (e.g. used help-desk working time) |

Table 11: Application Practices of Satisfactory Operation with possible metrics

The similarly established “Usefulness” and “Efficiency” metrics for the other (Information Integrity and Data Protection) governance practices can help management to develop management assertions by selecting governance practices as risk criteria for the Reliability Goals.

By this way only those governance practices are scoped as capability indicators evidencing achievement of specific governance outcomes (Process Performance attribute), which are considered by the management as relevant based on its risk appetite. This consideration might be “instinctive” or even “conscious” by following the Managing Operational Risks scenario.

Managed capability (level 2) scoping takes client’s pay-off or contractual period based metrics into context of longer term budget planning or reporting periods, which allows to perform trend analysis of historical data sourcing from multiple operational instances and periods.

Significant or dramatic (material) deviations from statistical trends indicate that internal or external risk factors should be reconsider followed by necessary actions in order to keep enterprise governance framework effective. This is why Managed capability - level 2 - scoping for governance processes is valid, as the wider/extended time-horizon and related objectives let management to use the performance metrics of the Managing Performance Reliability scenario as early success or failure indicators of achieving business unit or organization level operational effectiveness goals.
For example the trend for increasing volume of unsolved problems raised by customers during pay-off periods may indicate lower overall client satisfaction rate in the future jeopardizing operational effectiveness of the business unit or organization. However, handling only individual instances of deviations may take potential seasonal or unique reasons out of consideration.

Typically a governance process - as defined by the Governance Model for Trusted Businesses - is not performed as an individual project. For example Satisfactory Operation is incorporated into lower level operational management of a service or product delivery (e.g. of an on-going payroll service project); Information Reliability and Data Protection are performed through external or internal IT service activities directly supporting the business operation. Therefore the Managed (level 2) capability of these governance processes is normally evidenced by Managing Operational Performance of core business processes and their supporting projects. Of course it is not a “must” to cover any governance objective by the Managing Operational Performance scenario (e.g. of a payroll service project), as it depends on management’s decision on scoping of governance capability levels.
4.4 Managing Operational Effectiveness

4.4.1 Context and Specific Learning Objectives of Managing Operational Effectiveness

The following figure presents role of the Managing Operational Effectiveness scenario in supporting of Enterprise Governance:

![Role of the Managing Operational Effectiveness scenario in Enterprise Governance](image)

In the context of Managing Operational Effectiveness, Enterprise Governance should focus on those issues which are considered as relevant for the following sample management problems:

1. My organization (business unit) provides services or products according to internal or external specifications by keeping delivery deadlines and quality requirements and satisfying customer needs, however with lower than expected profitability.

2. Investment and development projects are not effective at business unit level. Delays and extra efforts cause higher expenditures than planned for the reporting periods.

3. Overheads and general expenses of business operation are too high.

4. Unexpected losses due to missing or redundant controls over operation.

5. Applied IT system is not aligned with quantitative and qualitative performance objectives of business operation.
6. Human resource competencies and their utilization are not sufficient in supporting business operation.

7. Design and operation of quality and control systems are not useful and/or effective.

Normally these issues are occurring and being managed in different time-scale than of the other Integrated Assurance Management scenarios. Managing Operational Performance is limited to the individual instances of the business processes and activities by considering service or product delivery requirements and schedule. Managing Performance Reliability considers contractual pay-off cycles with parallel or reoccurring business operational cycles, while Managing Operational Effectiveness typically has the time-horizon of the budgeting or reporting periods. Managing Strategic Directions is focusing on longer perspectives.

Operational Risk Management takes each governance objective into its specific time-horizon when setting risk criteria and measurable risk levels for selecting treatment options and evaluating their effectiveness.

Any reoccurring deviation from entity (business unit) level operational effectiveness objectives like profitability and agile resource allocation (rates per reporting periods) will call the management’s attention to check whether lower level Operational Performance and Reliable Operation objectives are adequately fulfilled as operational performance and reliability failures might also cause organizational level effectiveness problems. Furthermore some operational performance and reliability metrics - like more than planned resource usage, frequent corrective actions, customer dissatisfaction or low capacity utilization within operational life-cycles - are going to be early indicators of effectiveness problems at entity (business unit) level. Most of the operational effectiveness issues are coming to surface only by closures of budgeting or reporting periods, so early indicators of Operational Performance and Reliable Operation will help management and the boards (where they exist) to be more proactively prepared.

In case of no root cause having been found at Managing Operational Performance and Managing Performance Reliability, then Exploitability, Process Integrity and Competency objectives and related governance practices should be assessed whether the selection of practices and their capability targets are aligned with the entity (business unit) level effectiveness goals or the implemented practices are achieving their target capability levels.

Reoccurring deviations from profitability and agile resource allocation objectives are early indicators of those Strategic Direction issues which might be identical only by reviewing strategic planning periods. Assessment and improvement of Exploitability, Process Integrity and Competency objectives related process capability profiles are necessary risk management actions not just enabling entity (business unit) level operational effectiveness but also driving to better alignment to Strategic Directions.

Management actions taken during even longer than a reporting period (e.g. covering more quarterly or yearly financial or management statements) to achieve Exploitability, Process Integrity and Competency objectives - together with the other governance objectives - should be monitored by the board or other supervisory bodies (or by equivalent functions of the entity), and adequate level of transparency to all of the stakeholders should be provided by management disclosures.

This part of the case study material is focusing on the Managing Operational Effectiveness scenario, which enables achievement of organizational goals such as profitability and agile resource allocation over operational performance.

By the support of this Integrated Assurance Management scenario, the organization:

- realizes optimal value from business operation;
• effectively designs and operates process-level controls relevant to the objectives of business operation, and processing integrity principle;

• makes sufficient skills and knowledge relevant for the objectives of business operation available and effectively used.

The enabling governance processes are:

• Exploitable Operation, adapting practices from Enterprise SPICE
• Process Control, adapting practices from COSO
• Control Competency, adapting practices from COSO

Applicable measures:

• Profitability ("usefulness")
  - Indicator: Operating Margin
  - Time-horizon: reporting or budget planning periods

• Agile Resource Allocation ("efficiency")
  - Indicator: Unit Cost
  - Time-horizon: reporting or budget planning periods

In this part of the case study related to Managing Operational Effectiveness scenario, the Exploitability, Process Integrity and Competency governance objectives are selected to provide applicable use cases for the following learning objectives:

• Which key risk and risk factors are mitigated by the governance objectives referred by
  o The Exploitable Operation application area aiming to **ensure that organization realizes optimal value from business operation.**
  o The Process Control (Integrity) application area aiming 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.**
  o The Control Competence application area aiming 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.**

• How to implement and evaluate application practices evidencing achievement of **Exploitability** governance objective through the following outcomes:
  o *Investments for business operation needs and business potentials are performed deliberately.*
  o *Project management practices are applied for business operation.*
  o *Quality management practices are applied for business operation.*

• How to implement and evaluate application practices evidencing achievement of **Process Integrity** governance objective through the following outcomes:
• Control activities over access, amendments, adjustments and other usage of business information are maintained systematically.

• Application and general IT controls are maintained.

• Process performance metrics are collected and evaluated.

• How to implement and evaluate application practices evidencing achievement of Competency governance objective through the following outcomes:
  
  • Recruitment, compensation and training activities are performed systematically.
  
  • Staff members are continually informed, feedbacks are periodically reviewed.
  
  • Competent individuals are retained in relation to the business operation, financial reporting and related oversight roles.
4.4.2 Selecting the Scope of the Management Assertions for Managing Operational Effectiveness

A consistent risk assessment should be performed as the first step to establish management assertions by linking business activities to applicable governance practices and capability profiles for supporting the relevant governance objectives.

By using the definition of risk as “effect of uncertainties on objectives”, during the Managing Operational Effectiveness scenario we have to identify the risk criteria (tolerances and appetite) for governance objectives which are related to the entity (business unit) level Operational Effectiveness goals. In terms of operational effectiveness we use the “Usefulness” and “Efficiency” measures for setting metrics in time-horizon of reporting (or budget planning) periods, for example:

- Profitability measured by operating margin
- Agile resource allocation measured by unit cost

For ensuring risk optimisation we need targets and tolerances e.g. measured by:

- Percentage of achieving operating margin for reporting periods and
- Variance from planned unit cost.

The effective business operation related Exploitability, Process Integrity and Competency governance objectives should have such risk criteria which are applicable to measure effective risk treatment for achieving profitability and agile resource allocation goals by applying governance practices. Applicable governance practices should be selected and implemented by considering their relevance to the above “Usefulness” and “Efficiency” measures.

If a lower level governance practice offered by the Governance Model has no significant relevance for the established entity (business unit) level Operational Effectiveness goals, then there will be no need to apply that. If management specifies a governance practice as relevant for managing effective business operation within the context of stakeholders’ needs, then the target capability profile for implementing the governance process will include it and will be used as risk criteria (risk appetite). Capability level target should be set aligned with the relevant Enterprise Goals, as in this case in accordance with entity (business unit) level Operational Effectiveness goals.

Entity (business unit) level Operational Effectiveness objectives (Organizational Goals) are common in each type of business operation. However related governance practices and their capability levels might differ in wide range. Effective small business units might run their operation without extensive implementation of project and quality management, process control or human resource management practices as the much lower overhead costs ensure either higher profitability or advantage of more competitive pricing. When business volume is growing with facing to new customer requirements and organizational changes, then the need for organizational investments and projects like applying new IT platforms, skills, and procedures, etc. will emerge. Managing these organizational assets is a challenge even for the more matured enterprises. Most of these efforts are very expensive and normally the success rate of organizational development investments and projects are far away from expectations. By using of the Managing Operational Effectiveness Integrated Assurance Management scenario, the management will be able to select and apply those governance practices which are relevant for improving or ensuring better entity (business unit) level operational effectiveness based on the reliable performance of the well-established business operations.
Either well running operational practices are used to define standard processes or designing new processes can help to improve operational performance at entity (business unit) level. **Exploitability, Process Integrity and Competency** objectives related governance practices contribute to develop - level 3 - Established capability of those core and supporting business processes which constitute baseline business operation by establishing their organizational contexts.

Selection and implementation of those governance practices which are offered by the **Governance Model for Trusted Businesses** for **Exploitability, Process Integrity and Competency** objectives should be driven by the management's usefulness and efficiency considerations. Therefore the optimal (meaningful) coverage of offered governance practices, together with a capability profile aiming higher (e.g. Level 2 - Managed or Level 3 - Established) requirements should be concluded by performing mature risk management practices.

For supporting risk assessment the following risk tables for the **Exploitability, Process Integrity and Competency** objectives can be used to understand key risk areas and applicable practices as risk responses:

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable Enterprise SPICE processes</th>
<th>Application Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunities are not exploited</td>
<td>Necessary investments are not taken</td>
<td>Investment needs and potentials are considered systematically</td>
<td>Investment Management (ESPICE)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Management inefficiently use resources</td>
<td>Systematic project management practices applied</td>
<td>Project Management (ESPICE)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Product or service quality is not ensured</td>
<td>Systematic quality management practices applied</td>
<td>Quality Assurance and Management (ESPICE)</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 12: Exploitability related risk areas

Missing opportunities when business might be growing means losses in competitiveness. However even in circumstances of sharp competition or market downturn, those practices which are supporting the right
balance of costs and benefits related to entity (business unit) level management of investments, projects and quality assurance should be applied to keep sustainability.

The implemented governance practices are tools for improving ability of the entity (business unit) to optimize allocation and usage of available resources for running business operation in expected quality. The selected governance practices provide implementation instances of the Exploitable Operation governance process enabling the achievement of the following outcomes:

- Investments for business operation needs and business potentials are performed deliberately.
- Project management practices are applied for business operation.
- Quality management practices are applied for business operation.

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

Table 13: Process Integrity related risk areas

Internal controls built in business processes and supporting systems are important elements of ensuring operational effectiveness by mitigating the downside risks (uncertainties having negative impact on business objectives). However these controls and control activities should be carefully designed, implemented and...
evaluated in context of the organizational goals. Some of them are defined as necessary outcomes of business process descriptions to fulfil regulatory or other compliance requirements. Entity level controls might be also defined as processes by applying COSO or COBIT reference models, which make ISO/IEC 15504 process assessment method applicable to evaluate effectiveness of control design (by determining capability gaps between target and assessed process profiles) and effectiveness of control operation (by determining control risk levels based on gap occurrences).

The selected governance practices provide implementation instances of the Process control governance process enabling the achievement of the following outcomes:

- Control activities over access, amendments, adjustments and other usage of business information are maintained systematically.
- Application and general IT controls are maintained.
- Process performance metrics are collected and evaluated.

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable COSO&amp;COBIT processes and GAPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff is unable to perform control tasks</td>
<td>Lack of skilled staff</td>
<td>Recruitment, compensation and training activities are performed systematically</td>
<td>Human Resources (COSO)</td>
</tr>
<tr>
<td></td>
<td>Staff members do not know procedures and processing requirements</td>
<td>Staff members are continually informed, feedbacks are periodically reviewed</td>
<td>Internal Communication (COSO)</td>
</tr>
<tr>
<td></td>
<td>Changes of Skills Requirements</td>
<td>Adequate human resource practices are determined and used</td>
<td>Governance (Financial Reporting) Competencies (COSO)</td>
</tr>
</tbody>
</table>

Table 14: Competency related risk areas

Management of human resources for ensuring availability of skilled staff supported by effective internal communication and skills development options is an indispensable element of achieving entity (business
unit) level business goals. Lack of well-trained and adequately informed people will interfere to exploit business opportunities, cause less flexibility in allocation of human capacity or request extra control efforts by the management.

The selected governance practices provide implementation instances of the Control Competency governance process enabling the achievement of the following outcomes:

- Recruitment, compensation and training activities are performed systematically.
- Staff members are continually informed, feedbacks are periodically reviewed.
- Competent individuals are retained in relation to the business operation, financial reporting and related oversight roles.

The set of applied governance practices and the target Process Capability Attributes comprise those risk criteria against the business performance should be assessed. Evaluation of Process Attribute Gaps (between target and assessed capability) provides measurement of residual risk status.
4.4.3 Applying Management Assertions for Managing Operational Effectiveness

Management assertions are setting links between the business processes (and activities) and the governance objective-driven processes (and base practices) offered by recognized reference models (like COSO, COBIT and Enterprise SPICE). Management should reflect to their own business goals and business environment’s expectations by setting target capability profiles for the customized governance objectives (risk appetite) and adequate quantitative control limits of tolerable deviations from Enterprise Goals (risk tolerance).

Governance Capability Assessment (Governance SPICE) methodology provides measurement framework for targeting and assessing effectiveness of governance processes (defined by ISO/IEC 15504 compliant reference models) in achievement of governance objectives, however it should be carefully considered at the assessment scope definition, that a governance process might be implemented and applied by more than one business processes (and their instances) within a business operational unit.

For example in the case of Process Integrity objective concerning to the Monthly Payroll Calculation business process, the management should determine the management and control activities necessary and sufficient to limit the negative consequences of the inherent business risk related to failures in manual or automatic processing of payroll related data and information.

Theoretically the management should apply a measure for determining direct impact on specific business goals, however at business process level this measure can’t derived directly from “natural” business measures like income, profitability, stock listing rate, market-share, etc. This problem could be resolved by targeting application of governance practices by the business process activities. The more relevant governance practices are applied; the negative consequences are the more likely minimized.

However the adequate structure of performance measurement helps to navigate over applicable governance practices (see Figure 4: Linking Governance Objectives to Enterprise Goals & Measures). The governance practices are enabling achievement of Enterprise Goals, so measurement related to achievement of governance objectives should support in-time status information regarding overall business performance. Furthermore the lower level operational or organizational goals and metrics should be established as enabling indicators for the above governance level.

By this way the appearing deficiencies to target measures of Managing Performance Reliability - e.g. bad satisfaction or capacity utilization rates in a payroll service payoff period - might be early indicators of possible failures at Managing Operational Effectiveness level - e.g. decreasing operating margin or increasing unit cost detected by closing reporting periods. Similarly the metrics indicating deviation from Organizational Goals call the attention for possible consequences in achievement of Strategic Business Goals at Managing Strategic Directions level - e.g. missing revenue and cash flow targets of the organization in longer perspective than the current reporting period.

For selecting and prioritizing governance practices offered by the reference models, the Managing Operational Effectiveness scenario offers “Usefulness” and “Efficiency” aspects of business performance. In case of Monthly Payroll Calculation business process, the operational effectiveness should enable profitability (measured by operating margin for reporting periods) and agile resource allocation (measured by unit cost).

These two types of metrics help to identify relevance and weight of applicable governance practices in supporting performance objectives. If lack or failure of a governance practice - by considering together with other existing governance practices - represents undesirable uncertainty on keeping “Usefulness” or “Efficiency” goals, then implementation or
improvement of the practice will be an adequate risk treatment option. If the lack or failure of a governance practice has no significant effect on Enterprise Goals - by considering together with other existing governance practices – this practice will be out of the scope of implementation and assurance. Performance measurement is needed to establish the concerning risk criteria and tolerance levels triggering immediate or scheduled management actions.

For example: a failure (performance gap) of COSO IFC.CA.IT Information Technology practices for Process Integrity governance objective in a payroll outsourcing service – extensively using IT-enabled solutions - causes undesirable uncertainty in achievement of expected operational effectiveness. Failures in e.g. IT operation, change management, security management, etc. might cause less effective staff performance (double entries, repeating activities, manual works or corrections) or other wasted resources and extra overhead costs. Lower profitability and extra need for resource allocation are early indicators of potential deviation from strategic business targets of the organization. In this case an identified performance gap at maintaining Information Technology controls triggers the management actions for process improvement related to the Process Integrity governance objective. Even if the payroll data processing is supported by external IT solution (e.g. payroll software, IT infrastructure), the relevance and importance of maintaining Information Technology controls will remain within the service provider’s responsibility. Even usage of well-reputed or certified IT service will not simplify the implementation of this governance practice, as access controls and end-user computing issues, data backups will remain in shared responsibility.

The lower level metrics like actual operational incomes and costs of used resources per reporting period should be assessed against company targets (or other reasonable benchmark) and measures over pre-established tolerances should trigger the (re)assessment of maintaining Information Technology governance practices. If the assessed performance gap is significant as effecting profitability or resource utilization by exceeding their tolerances, then improvement action should be planned and implemented by the management. If detected performance gaps were not affecting significantly the Operational Effectiveness goals of payroll service unit, then either the triggering tolerances of lower level performance metrics might be reset, or - more likely - other related governance practices should be also assessed. Relevance and weight of a governance practice should be considered not just as an enabler of the related governance objective (e.g. maintaining Information Technology controls enables achievement of Operational Effectiveness goals), but also as whether its implementation would have effect on the next level Enterprise Goals. E.g. Maintaining Information Technology controls shouldn’t cost more than reasonable in context of Strategic Business Goals at Managing Strategic Directions level (might be measured by business revenue and cash flow figures).

At corporate level the governance objectives related set of practices comprising ISO/IEC 15504 compliant governance processes - as defined by the Governance Model - are applicable for targeting and assessing them for even higher (e.g. level 2 or above) governance capability. However from the selected business process view, as in the case of Monthly Payroll Calculation, the assessment target is mostly limited to Compliance (1 - Performed) level, as this is the level where the application of specific process outcomes and practices are investigated.

Targeting the Managed (level 2) or even higher level for the governance processes is applicable in the case when capability target of the Managing Operational Effectiveness scenario were pre-established accordingly (e.g. in compliance with strict regulatory requirements). The higher capability request for Managing Operational Effectiveness should be determined by the Operational Risk Management function and also takes other effected business units (e.g. not just the Payroll Service Unit, but others like the Sales, IT Development, etc. units) into the same capability level context.
4.4.4 Selecting specific application practices as risk criteria for Operational Effectiveness Goals

For fully achieving Process Performance attribute, the following specific outcomes should be evidenced concerning to the governance processes supporting Operational Effectiveness at business unit level (e.g. Payroll Service Unit):

- for Exploitable Operation governance process:
  - Investments for business operation needs and business potentials are performed deliberately.
  - Project management practices are applied for business operation.
  - Quality management practices are applied for business operation.

- for Process Control governance process:
  - Control activities over access, amendments, adjustments and other usage of business information are maintained systematically.
  - Application and general IT controls are maintained.
  - Process performance metrics are collected and evaluated.

- for Control Competence governance process:
  - Recruitment, compensation and training activities are performed systematically.
  - Staff members are continually informed, feedbacks are periodically reviewed.
  - Competent individuals are retained in relation to the business operation, financial reporting and related oversight roles.

The applied Governance Model for Trusted Businesses offers recognized best practices supporting these outcomes, however not all of them are necessary in context of the specific Enterprise Goals of the organization. Management should select only those practices as assertions, which have evidential link to “Usefulness” and “Efficiency” goals at this operational level. For Managing Operational Effectiveness of Payroll Service these goals are: reasonable profitability and effective resource allocation.

For careful consideration, management should set metrics like described in the following sample table. Where current metrics show significant deviation from management’s expectations (risk appetite), the related practice should be implemented or improved. Where current metrics are available and satisfactory to reasonable risk appetite, the application practice can be set for management assertion.

Next table shows sample metrics for application practices supporting Exploitability governance objective:
<table>
<thead>
<tr>
<th>Application Practices for Exploitability Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manage investments supporting business goals and targets.</strong> 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.</td>
<td>Income or savings generated by investment activities made with surplus cash (e.g. earnings on accounts, shares, securities, assets, etc. or benefits from other projects being out of the usual line of business)</td>
<td>Return of investment per investment types (e.g. return on cash savings, shares, securities, assets, etc. or projects being out of the usual line of business)</td>
</tr>
<tr>
<td><strong>GVM.2.BP1: Establish Criteria.</strong> Establish and maintain criteria for selecting and evaluating potential investments.</td>
<td>Coverage of investment types by income/savings targets (e.g. criteria for accounts, shares, securities, assets, projects, etc.)</td>
<td>Coverage of investment types by ROI targets (e.g. criteria for interest rates, return on shares, securities, assets, projects, etc.)</td>
</tr>
<tr>
<td><strong>GVM.2.BP2: Identify Investment Proposals.</strong> Collect business cases, identifying and describing investment proposals.</td>
<td>Coverage of investment types by comparable proposals (e.g. options of accounts, shares, securities, assets, projects, etc.)</td>
<td>Coverage of investment types by business case evaluations (e.g. industry benchmark for interest rate, return on shares, securities, assets, projects, etc.)</td>
</tr>
<tr>
<td><strong>GVM.2.BP3: Categorize Proposals.</strong> Define investment categories, categorization criteria, and categorize proposals.</td>
<td>Coverage of investment types by categorization criteria (e.g. categorization criteria for accounts, shares, securities, assets, projects, etc.)</td>
<td>Coverage of investment types by formal categorization (e.g. number of used categories for interest rate, return on shares, securities, assets, projects, etc.)</td>
</tr>
<tr>
<td><strong>GVM.2.BP4: Prioritize and Evaluate Investment Proposals.</strong> Evaluate and prioritize investment proposals.</td>
<td>Coverage of investment types by prioritization (e.g. frequency of prioritization for accounts, shares, securities, assets, projects, etc.)</td>
<td>Coverage of investment types by formal evaluation (e.g. frequency for evaluating options for interest rate, return on shares, securities, assets, projects, etc.)</td>
</tr>
<tr>
<td><strong>GVM.2.BP5: Establish and Maintain the Investment Portfolio.</strong> Select proposals to be included in the investment portfolio. Establish and maintain the investment portfolio.</td>
<td>Coverage of investment types by investment portfolio (e.g. coverage of)</td>
<td>Coverage of investment types by portfolio maintenance (e.g. frequency of portfolio)</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Application Practices for Exploitability</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance Objective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GVM.2.BP6: Identify and Allocate Resources. Allocate resources to execute selected investments. Reallocate resources from deactivated and terminated investments.</td>
<td>accounts, shares, securities, assets, projects, etc.)</td>
<td>maintenance per investment types)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of investment types by resource allocation and reallocation (e.g. frequency of allocating or reallocating resources per investment types)</td>
<td>Unexpected expenses or losses due to resource allocation or reallocation (e.g. resource allocation expenses or losses per investment types)</td>
</tr>
<tr>
<td>GVM.2.BP8: Adjust Investment Portfolio. Adjust the investment portfolio in response to actual portfolio performance.</td>
<td>Coverage of investment types by portfolio adjustment (e.g. frequency of portfolio adjustment per investment types)</td>
<td>Unexpected expenses or losses due to portfolio adjustment (e.g. portfolio adjustment expenses or losses per investment types)</td>
</tr>
<tr>
<td>GVM.2.BP9: Communicate Portfolio Adjustment. Communicate results of portfolio adjustment to relevant stakeholders.</td>
<td>Coverage of investment types by communicating portfolio adjustments (e.g. frequency of portfolio adjustment communication per investment types)</td>
<td>Unexpected costs due to communication of portfolio adjustments (e.g. extraordinary costs of portfolio adjustment communication per investment types)</td>
</tr>
<tr>
<td>GVM.2.BP10: Monitor Changes. Monitor changes in strategy, risk levels, and resource constraints to assure appropriate alignment.</td>
<td>Coverage of investment types by monitoring (e.g. number of monitoring indicators per investment types)</td>
<td>Unexpected costs of monitoring (e.g. extra monitoring efforts and costs per investment types)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of business unit level profitability goals by managed business activities/projects (e.g. rate of business unit operating profit coming from activities without project management)</td>
<td>Coverage of business unit level resource allocation by managed business activities/projects (e.g. rate of resources allocated to business operation without project</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Application Practices for Exploitatibility Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Coverage of business unit level profitability goals by all projects’ objectives (e.g. rate of organizational goals not supported by project objectives)</td>
<td>Coverage of business unit level resource allocation by all projects’ objectives (e.g. rate of staff resources allocated without mapping to project objectives)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of business unit level profitability goals by all projects’ life-cycle considerations (e.g. year-end closing project are not considered)</td>
<td>Coverage of business unit level resource allocation by all projects’ life-cycle considerations (e.g. year-end closing project resources are in conflict with parallel monthly services)</td>
</tr>
<tr>
<td>GVM.8.BP3: Define Stakeholders. Identify stakeholders and interfaces between project elements and with other project and organizational units.</td>
<td>Coverage of business unit level profitability goals by all projects’ stakeholder identification (e.g. IT support is not identified as stakeholder)</td>
<td>Coverage of business unit level resource allocation by considering all projects’ stakeholders needs (e.g. stakeholders involvement on other projects are not considered)</td>
</tr>
<tr>
<td>GVM.8.BP4: Estimate Planning Parameters. Estimate and document the work product and task planning parameters that provide a basis for resource estimates.</td>
<td>Coverage of business unit level profitability goals by all projects’ planning parameters (e.g. parameters of work products and work flows are mapped to organizational profitability goals)</td>
<td>Coverage of business unit level resource allocation by considering all projects’ planning parameters (e.g. resource estimates are only partially used)</td>
</tr>
<tr>
<td>GVM.8.BP5: Estimate Project Resource Requirements. Estimate the project effort, cost, schedule and other resource requirements.</td>
<td>Coverage of business unit level profitability goals by all projects’ resource requirements (e.g. profitability goals are considered based on estimating resource requirements by projects)</td>
<td>Coverage of business unit level resource allocation by all projects’ resource requirements (e.g. rate of allocated resources per running projects’ needs)</td>
</tr>
<tr>
<td>GVM.8.BP6: Establish Schedules. Develop schedules for the project.</td>
<td>Coverage of business unit level profitability goals by all projects’ schedules (e.g.</td>
<td>Coverage of business unit level resource allocation by all projects’ schedules (e.g. rate of...</td>
</tr>
</tbody>
</table>
## Application Practices for Exploitation Governance Objective

<table>
<thead>
<tr>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>profitability goals and schedule of all projects’ results are aligned</td>
<td>available resources according to all projects’ schedules</td>
</tr>
<tr>
<td>Coverage of business unit level profitability goals by all projects’ budgets (e.g. profitability goals and project budgets are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ budgets (e.g. rate of available resources according to project budgets)</td>
</tr>
<tr>
<td>Coverage of business unit level profitability goals by all projects’ quality/compliance requirements (e.g. profitability goals and all projects’ quality/compliance requirements are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ quality/compliance requirements (e.g. rate of available qualified resources according to all projects’ quality/compliance requirements)</td>
</tr>
<tr>
<td>Coverage of business unit level profitability goals by all projects’ human resource requirements (e.g. profitability goals and all projects’ human resources requirements are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ human resource requirements (e.g. rate of available skills and competencies according to all projects’ requirements)</td>
</tr>
<tr>
<td>Coverage of business unit level profitability goals by all projects’ communication requirements (e.g. profitability goals and all projects’ communication requirements are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ communication requirements (e.g. rate of available communication resources according to all projects’ requirements)</td>
</tr>
<tr>
<td>Coverage of business unit level profitability goals by all projects’ risk considerations (e.g. profitability goals and all projects’ risk)</td>
<td>Coverage of business unit level resource allocation by all projects’ risk considerations (e.g. rate of available risk management resources)</td>
</tr>
</tbody>
</table>

**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.

---

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Application Practices for Exploitability</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GVM.8.BP12: Plan Procurements.</strong> Plan and document project purchasing decisions.</td>
<td>Coverage of business unit level profitability goals by all projects’ procurements needs (e.g. profitability goals and all projects’ procurement needs are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ procurement needs (e.g. rate of available purchasing resources according to all projects’ needs)</td>
</tr>
<tr>
<td><strong>GVM.8.BP13: Establish and Maintain Plans.</strong> Establish and maintain a complete set of plans for providing the products and services throughout the project life cycle.</td>
<td>Coverage of business unit level profitability goals by all projects’ plans (e.g. profitability goals and all projects’ plans are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ plans (e.g. rate of available resources according to all projects’ needs)</td>
</tr>
<tr>
<td><strong>GVM.8.BP14: Establish Commitment.</strong> Establish and maintain commitment of affected groups and individuals to project objectives and plans and commitment of resources as identified in the plan.</td>
<td>Coverage of business unit level profitability goals by all projects’ commitment statements (e.g. profitability goals and all projects’ commitment statements are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ commitment statements (e.g. rate of resources under scope of all projects’ commitment statements)</td>
</tr>
<tr>
<td><strong>GVM.8.BP15: Acquire, Develop and Manage Project Team.</strong> 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.</td>
<td>Coverage of business unit level profitability goals by all projects’ authorisations and responsibilities (e.g. profitability goals and all projects’ authorisation and responsibilities are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ authorisations and responsibilities (e.g. rate of fulfilled positions and responsibilities according to all projects’ requirements)</td>
</tr>
<tr>
<td><strong>GVM.8.BP16: Direct and Manage Project Execution.</strong> Perform the work defined in the project plan to achieve the project’s objectives.</td>
<td>Coverage of business unit level profitability goals by all projects’ executions (e.g. profitability goals and all projects’ executions are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ executions (e.g. rate of available resources according to all projects’ executions)</td>
</tr>
<tr>
<td><strong>GVM.8.BP17: Distribute Information.</strong> Make relevant or established information available</td>
<td>Coverage of business unit level profitability goals by all projects’</td>
<td>Coverage of business unit level resource allocation by all projects’</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Application Practices for Exploitability Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>to project stakeholders as planned.</td>
<td>information needs (e.g. profitability goals and all projects’ information needs are aligned)</td>
<td>information needs (e.g. rate of available resources according to satisfy all projects’ information needs)</td>
</tr>
<tr>
<td><strong>GVM.8.BP18: Manage Stakeholder Expectations.</strong> Communicate and work with stakeholders to meet their needs and address issues as they occur.</td>
<td>Coverage of business unit level profitability goals by all projects’ stakeholder needs (e.g. profitability goals and all projects’ stakeholder needs are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ stakeholder needs (e.g. rate of available resources according to satisfy all projects’ stakeholder needs)</td>
</tr>
<tr>
<td><strong>GVM.8.BP19: Monitor Project Performance.</strong> Monitor and track project activities and results against plans and baseline.</td>
<td>Coverage of business unit level profitability goals by all projects’ performance monitoring (e.g. profitability goals and all projects’ performance monitoring are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ performance monitoring needs (e.g. rate of available resources according to all projects’ performance monitoring needs)</td>
</tr>
<tr>
<td><strong>GVM.8.BP20: Review and Analyze Project Performance.</strong> Conduct formal and informal reviews of project performance and analyze variances from the plans.</td>
<td>Coverage of business unit level profitability goals by all projects’ performance reviews (e.g. profitability goals and all projects’ performance reviews are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ performance review needs (e.g. rate of available resources according to all projects’ performance review needs)</td>
</tr>
<tr>
<td><strong>GVM.8.BP21: Take Corrective Action.</strong> Take corrective actions to address problems</td>
<td>Coverage of business unit level profitability goals by all projects’ corrective actions (e.g. profitability goals and all projects’ corrective actions are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ correction needs (e.g. rate of available resources according to all projects’ correction needs)</td>
</tr>
<tr>
<td><strong>GVM.8.BP22: Close Project.</strong> Close the project formally using appropriate organizational mechanisms and update organizational process assets</td>
<td>Coverage of business unit level profitability goals by all projects’ closures (e.g. profitability goals and all projects’ closure mechanism are aligned)</td>
<td>Coverage of business unit level resource allocation by all projects’ closures (e.g. rate of available resources according to all projects’ closure activities)</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Application Practices for Exploitability Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Coverage of business unit level profitability goals by quality management and assurance of business operation (e.g. rate of business unit operating profit coming from activities without quality management controls)</td>
<td>Coverage of business unit level resource allocation by quality management and assurance of business operation (e.g. rate of resources allocated to business operation without project management controls)</td>
</tr>
<tr>
<td>SUP.3.BP1: Establish a Quality Management System. Establish, document, implement, and maintain a quality management system.</td>
<td>Coverage of business unit level profitability goals by quality management (e.g. rate of profitability goals aligned with quality management objectives)</td>
<td>Coverage of business unit level resource allocation by quality management (e.g. rate of available resources according to quality management needs)</td>
</tr>
<tr>
<td>SUP.3.BP2: Monitor Process Compliance. Objectively monitor compliance of performed activities with the established processes.</td>
<td>Coverage of business unit level profitability goals by compliance monitoring (e.g. profitability goals and compliance monitoring are aligned)</td>
<td>Coverage of business unit level resource allocation by compliance monitoring needs (e.g. rate of available resources according to compliance monitoring needs)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of business unit level profitability goals by monitoring product and service quality (e.g. profitability goals and quality monitoring are aligned)</td>
<td>Coverage of business unit level resource allocation by quality monitoring needs (e.g. rate of available resources according to quality monitoring needs)</td>
</tr>
<tr>
<td>SUP.3.BP4: Monitor Noncompliance Issues. Monitor and track noncompliance issues and support their resolution via escalation to senior management if necessary.</td>
<td>Coverage of business unit level profitability goals by monitoring noncompliance issues (e.g. profitability goals and resolution of noncompliance issues are aligned)</td>
<td>Coverage of business unit level resource allocation by monitoring noncompliance issues (e.g. rate of available resources according to resolution of noncompliance issues)</td>
</tr>
<tr>
<td>SUP.3.BP5: Record and Report Results. Record and report the results of quality assurance activities and customer satisfaction data to applicable stakeholders.</td>
<td>Coverage of business unit level profitability goals by quality records and reports</td>
<td>Coverage of business unit level resource allocation by quality assurance (e.g. rate of...</td>
</tr>
</tbody>
</table>
### Table 15: Application Practices of Exploitable Operation with possible metrics

<table>
<thead>
<tr>
<th>Application Practices for Exploitability Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUP.3.BP6: Analyze Quality.</strong> Analyze quality records and measurements to detect the need for corrective action and develop recommendations for quality improvement or corrective and preventive actions.</td>
<td>(e.g. profitability goals and quality assurance results are aligned)</td>
<td>available resources according to quality assurance needs)</td>
</tr>
<tr>
<td><strong>SUP.3.BP7: Initiate Quality Improvement.</strong> Initiate activities that address identified quality issues or quality improvement opportunities.</td>
<td>Coverage of business unit level profitability goals by quality analysis (e.g. profitability goals and quality analysis are aligned)</td>
<td>Coverage of business unit level resource allocation by quality analysis (e.g. rate of available resources according to quality analysis needs)</td>
</tr>
<tr>
<td><strong>SUP.3.BP8: Monitor and Evaluate the Effect of Changes.</strong> Monitor the status of quality improvements on products and services and evaluate the effect of changes after they have been implemented.</td>
<td>Coverage of business unit level profitability goals by monitoring of quality improvement (e.g. profitability goals and monitoring of quality improvement actions are aligned)</td>
<td>Coverage of business unit level resource allocation by monitoring of quality improvements (e.g. rate of available resources according to monitoring needs of quality improvement)</td>
</tr>
</tbody>
</table>

The similarly established “Usefulness” and “Efficiency” metrics for the other (Process Control and Control Competence) governance practices can help management to develop management assertions by selecting governance practices as risk criteria for the Operational Effectiveness goals.

By this way only those governance practices are scoped as capability indicators evidencing achievement of specific governance outcomes (Process Performance attribute), which are considered by the management as relevant based on its risk appetite. This consideration might be “instinctive” or even “conscious” by following the Managing Operational Risks scenario.

Managed capability (level 2) scoping takes budget planning or reporting period based metrics into context of longer strategic planning periods, which allows performing trend analysis of historical data sourcing from multiple reporting data and periods.

Significant or dramatic (material) deviations from strategic plans indicate that internal or external risk factors should be reconsider followed by necessary actions in order to keep enterprise governance framework effective. This is why Managed capability - level 2 - scoping for governance processes is valid, as the wider/extended time-horizon and related objectives let management to use the performance metrics of the Managing Operational Effectiveness scenario as early success or failure indicators of achieving strategic business goals.
For example the trend for decreasing operating margin or increasing unit cost may indicate lower operational effectiveness of the business unit or organization in the future jeopardizing business sustainability. However, handling only individual instances of deviations may take potential seasonal or unique reasons out of consideration.

Typically a governance process - as defined by the Governance Model for Trusted Businesses - is not performed as an individual project. For example Exploitable Operation is incorporated into organizational management of a business unit (e.g. Payroll Service Unit); Process Control and Control Competence are performed through business unit management activities directly supporting the business operation. Therefore the Managed (level 2) capability of these governance processes is normally evidenced by business unit management activities and their supporting projects.
4.5 Managing Strategic Directions

4.5.1 Context and Specific Learning Objectives of Managing Strategic Directions

The following figure presents role of the Managing Strategic Directions scenario in supporting of Enterprise Governance:

![Diagram](image)

Figure 17: Role of the Managing Strategic Directions scenario in Enterprise Governance

In the context of **Managing Strategic Directions**, Enterprise Governance should focus on those issues which are considered as relevant for the following sample management problems:

1. My company runs successful business operation(s) with expected profitability; however the organization is not proactive enough to react well to the rapidly changing business environment and market demands.

2. Due to changing or new client requirements and growing competition our business offers and proposals are not received as well as in past.

3. New business operation (service or product) start-up is in progress which requests new organizational structures and procedures.

4. Increasing volume of business operation request more robust business continuity planning.

5. Changes in business volume need to explore new funding solutions by extensive communications with external parties.
6. New shareholders, investors request more transparency and management accountability over running business operation(s).

7. Stakeholders request attestation and public disclosures of business excellence.

Normally these issues are occurring and being managed in different time-scale than of the other Integrated Assurance Management scenarios. Managing Operational Performance is limited to the individual instances of the business processes and activities by considering service or product delivery requirements and schedule. Managing Performance Reliability considers contractual pay-off cycles with parallel or reoccurring business operational cycles, while Managing Operational Effectiveness typically has the time-horizon of the budgeting or reporting periods. Managing Strategic Directions is focusing on longer perspectives. Operational Risk Management takes each governance objective into its specific time-horizon when setting risk criteria and measurable risk levels for selecting treatment options and evaluating their effectiveness.

Any reoccurring deviation from company level strategic business objectives like achieving business goals and availability of funding resources (indicators for strategic planning periods) will call the management's attention to check whether lower level Operational Performance, Reliable Operation and Operational Effectiveness objectives are adequately fulfilled as operational performance, reliability and entity/business unit level effectiveness failures might also cause problems in achieving strategic objectives. Furthermore some operational performance, reliability and effectiveness metrics - like more than planned resource usage, frequent corrective actions, customer dissatisfaction, low capacity utilization within operational life-cycles and decreasing operating margin or increasing unit costs during reporting periods - are going to be early indicators of problems in achieving strategic business objectives at company level. Most of the strategic issues are coming to surface only by reviewing or closing strategic planning periods, so early indicators of Operational Performance, Reliable Operation and Operational Effectiveness will help management and the boards (where they exist) to be more proactively prepared to strategic challenges.

In case of no root cause having been found at Managing Operational Performance, Managing Performance Reliability and Managing Operational Effectiveness, then Competitiveness, Accountability and Commitment objectives and related governance practices should be assessed whether the selection of practices and their capability targets are aligned with the company level strategic goals or the implemented practices are achieving their target capability levels.

Reoccurring deviations from profitability and agile resource allocation objectives are early indicators of those Strategic Direction issues which might be identical only by reviewing strategic planning periods. Assessment and improvement of Competitiveness, Accountability and Commitment objectives related process capability profiles are necessary risk management actions enabling better alignment to Strategic Directions.

Management actions taken during strategic planning period to achieve Competitiveness, Accountability and Commitment objectives - together with the other governance objectives - should be monitored by the board or other supervisory bodies (or by equivalent functions of the entity), and adequate level of transparency to all of the stakeholders should be provided by management disclosures.

This part of the case study material is focusing on the Managing Strategic Directions scenario, which enables achievement of strategic objectives such as achieving business goals and availability of funding resources.

By the support of this Integrated Assurance Management scenario, the organization is enabled:

- to ensure market recognition of the business operation;
• 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;

• to ensure that the organization and its staff are committed to comply with ethical and integrity requirements relevant to the objectives of financial reporting and trusted business operation, and availability principle.

The enabling governance processes are:

• Competitive Operation, adapting practices from Enterprise SPICE
• Control Management, adapting practices from COSO
• Control Competency, adapting practices from COSO and COBIT

Applicable measures:

• Business Goals ("usefulness")
  - Indicator: Revenues
  - Time-horizon: strategic planning periods

• Funding Resources ("efficiency")
  - Indicator: Cash Flow
  - Time-horizon: strategic planning periods

In this part of the case study related to Managing Strategic Directions scenario, the Competitiveness, Accountability and Commitment governance objectives are selected to provide applicable use cases for the following learning objectives:

• Which key risk and risk factors are mitigated by the governance objectives referred by
  o The Competitive Operation application area aiming to ensure market recognition of the business operation.
  o The Control Management (Accountability) application area aiming 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.
  o The Integrity Assurance (Commitment) application area aiming to ensure that the organization and its staff are committed to comply with ethical and integrity requirements relevant to the objectives of financial reporting and trusted business operation, and availability principle.

• How to implement and evaluate application practices evidencing achievement of Competitiveness governance objective through the following outcomes:
  o Business goals and targets are systematically maintained.
  o Customers and other stakeholder needs and expectations are considered for improvement of product or service features.
  o Effective proposal preparation practices are maintained.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
• How to implement and evaluate application practices evidencing achievement of **Accountability** governance objective through the following outcomes:
  
  o *Policies and procedures relevant for the governance objectives of financial reporting and trusted business operation are consistently implemented and communicated.*
  
  o *Management structure is adequate to internal control over financial reporting and trusted business operation.*
  
  o *Management takes stimulating behavior for supporting internal control over financial reporting and trusted business operation.*

• How to implement and evaluate application practices evidencing achievement of **Commitment** governance objective through the following outcomes:
  
  o *Ethical values are articulated and kept.*
  
  o *Active policies and procedures are in place to ensure business continuity.*
  
  o *Information from external parties are collected and reviewed systematically.*
4.5.2 Selecting the Scope of the Management Assertions for Managing Strategic Directions

A consistent risk assessment should be performed as the first step to establish management assertions by linking business activities to applicable governance practices and capability profiles for supporting the relevant governance objectives.

By using the definition of risk as “effect of uncertainties on objectives”, during the Managing Strategic Directions scenario we have to identify the risk criteria (tolerances and appetite) for governance objectives which are related to the company level Strategic Directions. In terms of strategic directions we use the “Usefulness” and “Efficiency” measures for setting metrics in time-horizon of strategic planning periods, for example:

- Business goals measured by revenues
- Funding resources measured by cash flow

For ensuring risk optimisation we need targets and tolerances e.g. measured by:

- Percentage of achieving revenue targets for strategic planning periods and
- Variance from planned cash flow.

The strategic directions related Exploitability, Process Integrity and Competency governance objectives should have such risk criteria which are applicable to measure effective risk treatment for achieving business goals and funding resources by applying governance practices. Applicable governance practices should be selected and implemented by considering their relevance to the above “Usefulness” and “Efficiency” measures.

If a lower level governance practice offered by the Governance Model has no significant relevance for the established company level Strategic Directions, then there will be no need to apply that. If management specifies a governance practice as relevant for managing strategic directions within the context of stakeholders’ needs, then the target capability profile for implementing the governance process will include it and will be used as risk criteria (risk appetite). Capability level target should be set aligned with the relevant Enterprise Goals, as in this case in accordance with company level Strategic Business goals.

Settings of Strategic Directions (Strategic Business Goals) are similar in each type of business organization. However related governance practices and their capability levels might differ in wide range. Effective small enterprises might run their business operation without extensive implementation of strategic planning, control management or integrity assurance practices. When business volume is growing with facing to new customer requirements and organizational changes, then the need for more formal strategic thinking, higher level of transparency and accountability together with commitment to business integrity and availability principles will emerge. Managing these needs according to expectations of the business environment and the stakeholders is a challenge even for the more matured enterprises. By using of the Managing Strategic Directions Integrated Assurance Management scenario, the management will be able to select and apply those governance practices which are relevant for improving or ensuring better market recognition, transparency and accountability of company management and commitment to business excellence.

Either well running management practices are used to define policies and procedures or designing new management processes can help to improve governance at company level. Competitiveness, Accountability and Commitment objectives related governance practices contribute to develop - level 3 - Established capability of those management processes which constitute management of business operation by establishing their organizational contexts.
Selection and implementation of those governance practices which are offered by the **Governance Model for Trusted Businesses** for Competitiveness, Accountability and Commitment objectives should be driven by the management's usefulness and efficiency considerations. Therefore the optimal (meaningful) coverage of offered governance practices, together with a capability profile aiming higher (e.g. Level 2 - Managed or Level 3 - Established) requirements should be concluded by performing mature risk management practices.

For supporting risk assessment the following risk tables for the **Competitiveness, Accountability and Commitment** objectives can be used to understand key risk areas and applicable practices as risk responses:

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable Enterprise SPICE processes</th>
<th>Application Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loosing Market</td>
<td>Market needs are not respected</td>
<td>Improvement of product or service features are considered periodically</td>
<td>Needs (ESPICE)</td>
<td>The organization applies practices to elicit, analyze, clarify, and document evolving customer and other stakeholder needs and expectations.</td>
</tr>
<tr>
<td></td>
<td>Business objectives are not reflecting to the changes of economic environment</td>
<td>Business goals and targets are systematically maintained</td>
<td>Enterprise Governance (ESPICE)</td>
<td>The organization applies practices to establish strategic enterprise direction and ensure the enterprise achieves its goals and objectives.</td>
</tr>
<tr>
<td>Business proposals are not convincing</td>
<td>Improvement of proposal preparation</td>
<td>Tendering (ESPICE)</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

Table 16: Competitiveness related risk areas

Loosing market during strategic time-horizon means danger for business sustainability. A short term impact is the decreasing value of the company (stock) jeopardizing working conditions of the management and the employees. For longer term the ownership structure of the company or the legal entity owning the business operation might be dramatically changed, or at worst case the business operation might be terminated.

The implemented governance practices are tools for improving ability of the company to refine its strategy and aligned business goals according to the changeable business environment and clients’ needs and to maintain successful proposal preparation practices to achieve sales targets. The selected governance
practices provide implementation instances of the **Competitive Operation** governance process enabling the achievement of the following outcomes:

- Business goals and targets are systematically maintained.
- Customers and other stakeholder needs and expectations are considered for improvement of product or service features.
- Effective proposal preparation practices are maintained.

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable COSO processes</th>
<th>Application Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management is unable to control business processes</td>
<td>No consistent or properly communicated policies and procedures</td>
<td>Policies and procedures are maintained and used in operation</td>
<td>Policies and Procedures (COSO)</td>
<td>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.</td>
</tr>
<tr>
<td>Management structure is inadequate</td>
<td>Management takes stimulating behaviour</td>
<td>Authority and Responsibility (COSO)</td>
<td>Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting and trusted business operation.</td>
<td></td>
</tr>
<tr>
<td>Management attitude is not exemplary</td>
<td>Management takes stimulating behaviour</td>
<td>Management’s Philosophy and Operating Style (COSO)</td>
<td>Management’s philosophy and operating style support achieving effective internal control over financial reporting and trusted business operation.</td>
<td></td>
</tr>
</tbody>
</table>

Table 17: Accountability related risk areas

Accountability of the management is evidently important for all stakeholders of the company. Normally the legal documents and the company law extended with the internal policies and procedures constitute the static environment for management accountability, however this should be also dynamic to effectively respond to the current needs or changes of the running business operation. Therefore the governance practices enabling effective management control of business operation should be selected and implemented.
not just according to legal requirements, but also in alignment with the strategic business objectives, the clients’ needs and the expectations of business environment.

The selected governance practices provide implementation instances of the **Control Management** governance process enabling the achievement of the following outcomes:

- Policies and procedures relevant for the governance objectives of financial reporting and trusted business operation are consistently implemented and communicated.
- Management structure is adequate to internal control over financial reporting and trusted business operation.
- Management takes stimulating behavior for supporting internal control over financial reporting and trusted business operation.

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable COSO&amp;COBIT processes</th>
<th>Application Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business integrity is not respectful</td>
<td>No commitment to ethical values</td>
<td>Ethical values are articulated and followed</td>
<td>Integrity and Ethical Values (COSO)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Interruption of information and communication systems</td>
<td>Active policies and procedures are in place to ensure business continuity</td>
<td>Ensure Continuous Service (COBIT)</td>
<td>Satisfy the business requirement of ensuring minimal business impact in the event of an IT service interruption.</td>
</tr>
<tr>
<td></td>
<td>External feedbacks and opinions are not considered</td>
<td>Information from external parties are collected and reviewed systematically</td>
<td>External Communication (COSO)</td>
<td>Matters affecting the achievement of the financial reporting and trusted business operation objectives are communicated with outside parties.</td>
</tr>
</tbody>
</table>

Table 18: Commitment related risk areas

Commitment to business ethics, integrity and availability (business continuity) principles is an important message to the market that the company management is aware of and manage reputation risks. The implementation of these principles are embedded in the effectively managed, reliable business operations, however company level attestation and communication of business excellence have additional value for the stakeholders. Companies might get advantages from not only mitigating reputation risks, but even increase...
their competitiveness by qualifying and presenting their strengths in governance and high capability profiles for trusted business operation.

The selected governance practices provide implementation instances of the **Integrity Assurance** governance process enabling the achievement of the following outcomes:

- Ethical values are articulated and kept.
- Active policies and procedures are in place to ensure business continuity.
- Information from external parties are collected and reviewed systematically.

The set of applied governance practices and the target Process Capability Attributes comprise those risk criteria against the business performance should be assessed. Evaluation of Process Attribute Gaps (between target and assessed capability) provides measurement of residual risk status.
4.5.3 Applying Management Assertions for Managing Strategic Directions

Management assertions are setting links between the business processes (and activities) and the governance objective-driven processes (and base practices) offered by recognized reference models (like COSO, COBIT and Enterprise SPICE). Management should reflect to their own business goals and business environment’s expectations by setting target capability profiles for the customized governance objectives (risk appetite) and adequate quantitative control limits of tolerable deviations from Enterprise Goals (risk tolerance).

**Governance Capability Assessment** (Governance SPICE) methodology provides measurement framework for targeting and assessing effectiveness of governance processes (defined by ISO/IEC 15504 compliant reference models) in achievement of governance objectives, however it should be carefully considered at the assessment scope definition, that a governance process might be implemented and applied by more than one business processes (and their instances) within a business operational unit.

For example in the case of **Accountability** objective concerning to the **Monthly Payroll Calculation** business process, the management should determine the management and control activities necessary and sufficient to limit the negative consequences of the inherent business risk related to the missing or inadequately defined company level policies and procedures, authorities and responsibilities over business operation; and related to the equivocal management behaviour. These organizational contexts of the specific process performance are enabled by fulfilling the Established - level 3 - capability requirements.

Theoretically the management should apply a measure for determining direct impact on specific business goals, however at business process level this measure can’t derived directly from “natural” business measures like income, profitability, stock listing rate, market-share, etc. This problem could be resolved by targeting application of governance practices by the business process activities. The more relevant governance practices are applied; the negative consequences are the more likely minimized.

However the adequate structure of performance measurement helps to navigate over applicable governance practices (see Figure 4: Linking Governance Objectives to Enterprise Goals & Measures). The governance practices are enabling achievement of Enterprise Goals, so measurement related to achievement of governance objectives should support in-time status information regarding overall business performance. Furthermore the lower level operational or organizational goals and metrics should be established as enabling indicators for the above governance level.

By this way the appearing deficiencies to target measures of **Managing Operational Effectiveness** - e.g. decreasing operating margin or increasing unit costs in a reporting period - might be early indicators of possible failures at **Managing Strategic Directions** level - e.g. missing the revenue targets or unbalanced cash flow detected by reviewing or closing strategic planning periods.

For selecting and prioritizing governance practices offered by the reference models, the **Managing Strategic Directions** scenario offers “Usefulness” and “Efficiency” aspects of business performance. In case of Payroll Service Operation, the alignment to strategic directions should enable achievement of **business goals** (measured by revenues for strategic planning periods) and availability of **funding resources** (measured by cash flow).

These two types of metrics help to identify relevance and weight of applicable governance practices in supporting performance objectives. If lack or failure of a governance practice - by considering together with other existing governance practices - represents undesirable uncertainty on keeping “Usefulness” or “Efficiency” goals, then implementation or improvement of the practice will be an adequate risk treatment option. If the lack or failure of
a governance practice has no significant effect on Enterprise Goals - by considering together with other existing governance practices – this practice will be out of the scope of implementation and assurance. Performance measurement is needed to establish the concerning risk criteria and tolerance levels triggering immediate or scheduled management actions.

For example: a failure (performance gap) of COSO IFC.CE.AR Authority and Responsibility practices for Accountability governance objective in a company running payroll outsourcing service – with sharing responsibilities over user organizations’ internal control - causes undesirable uncertainty in achievement of recognition as excellent and trusted business partner. Failures in e.g. in defining management and staff responsibilities, authorities and empowerment might cause reputational damages and loosing competitiveness leading to potential deviation from strategic business targets of the organization. In this case an identified performance gap at maintaining Authority and Responsibility controls triggers the management actions for process improvement related to the Accountability governance objective. External requirements for the service organizations controls over payroll service - like SOC 1 and SOC 2 – emphasize the relevance and importance of maintaining Authority and Responsibility controls.

The lower level metrics like coverage of business operation (relevant for achieving business goals and effectively using funding resources) by defined and assigned authorities and responsibilities should be assessed against company targets (or other reasonable benchmark) and measures over pre-established tolerances should trigger the (re)assessment of Authority and Responsibility governance practices. If the assessed performance gap is significant as affecting revenue or cash flow targets by exceeding their tolerances, then improvement action should be planned and implemented by the management. If detected performance gaps were not affecting significantly the Strategic Business Goals of the company running payroll service, then either the triggering tolerances of lower level performance metrics might be reset, or - more likely - other related governance practices should be also assessed. Relevance and weight of a governance practice should be considered as an enabler of the related governance objective (like maintaining Authority and Responsibility controls enables achievement of Accountability objective supporting Strategic Business Goals).

At corporate level the governance objectives related set of practices comprising ISO/IEC 15504 compliant governance processes - as defined by the Governance Model - are applicable for targeting and assessing them for even higher (e.g. level 2 or above) governance capability. However from the selected business process view, as in the case of Monthly Payroll Calculation, the assessment target is mostly limited to Compliance (1 - Performed) level, as this is the level where the application of specific process outcomes and practices are investigated.

Targeting the Managed (level 2) or even higher level for the governance processes is applicable in the case when capability target of the Managing Strategic Directions scenario were pre-established accordingly (e.g. in compliance with strict regulatory requirements). The higher capability request for Managing Strategic Directions should be determined by the Operational Risk Management function and also takes other effected business units (e.g. not just the Payroll Service Unit, but others like the Sales, IT Development, etc. units) into the same capability level context.
4.5.4 Selecting specific application practices as risk criteria for Strategic Directions

For fully achieving Process Performance attribute, the following specific outcomes should be evidenced concerning to the governance processes supporting Strategic Directions at company level (e.g. Payroll Service Company):

- for Competitive Operation governance process:
  - Business goals and targets are systematically maintained.
  - Customers and other stakeholder needs and expectations are considered for improvement of product or service features.
  - Effective proposal preparation practices are maintained.

- for Control Management governance process:
  - Policies and procedures relevant for the governance objectives of financial reporting and trusted business operation are consistently implemented and communicated.
  - Management structure is adequate to internal control over financial reporting and trusted business operation.
  - Management takes stimulating behavior for supporting internal control over financial reporting and trusted business operation.

- for Integrity Assurance governance process:
  - Ethical values are articulated and kept.
  - Active policies and procedures are in place to ensure business continuity.
  - Information from external parties are collected and reviewed systematically.

The applied Governance Model for Trusted Businesses offers recognized best practices supporting these outcomes, however not all of them are necessary in context of the specific Enterprise Goals of the organization. Management should select only those practices as assertions, which have evidential link to “Usefulness” and “Efficiency” goals at this operational level. For Managing Strategic Directions of a Payroll Service Company these goals are: achieving revenue target and available funding resources.

For careful consideration, management should set metrics like described in the following sample table. Where current metrics show significant deviation from management’s expectations (risk appetite), the related practice should be implemented or improved. Where current metrics are available and satisfactory to reasonable risk appetite, the application practice can be set for management assertion.

Next table shows sample metrics for application practices supporting Competitiveness governance objective:
<table>
<thead>
<tr>
<th>Application Practices for Competitiveness Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Establish and maintain business goals and targets.</strong> The organization applies practices to establish strategic enterprise direction and ensure the enterprise achieves its goals and objectives.</td>
<td>Revenue targets per business operations in planning and reporting time horizons aligned with strategy (e.g. monthly, yearly, etc. sales targets of payroll service)</td>
<td>Availability of funding resources per business operations in planning and reporting time horizons aligned with strategy (e.g. monthly, yearly, etc. cash flow targets of payroll service)</td>
</tr>
<tr>
<td><strong>GVM.1.BP1: Establish and Maintain Strategic Vision.</strong> Establish, maintain, and communicate a strategic vision that identifies long-term goals, values, performance expectations, and core activities.</td>
<td>Long term revenue targets per business operations (e.g. sales target for the next 3 years for payroll service)</td>
<td>Long term targets for operating and non-operating cash flow (e.g. rate of operating cash flow within total funding in the next 3 years for payroll service)</td>
</tr>
<tr>
<td><strong>GVM.1.BP2: Establish and Maintain Policies.</strong> Establish, maintain and communicate policies and directives.</td>
<td>Coverage of business operations by governance policies and directives (e.g. implementing 11 governance objectives for payroll service)</td>
<td>Coverage of business operations by funding policies (e.g. no external funding for payroll service operation planned in the next period)</td>
</tr>
<tr>
<td><strong>GVM.1.BP3: Align to Achieve the Vision.</strong> 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.</td>
<td>Coverage of business units by governance policies and directives (e.g. implementing 11 governance objectives for all business units)</td>
<td>Coverage of business units by funding policies (e.g. no external funding for payroll service unit and supporting IT department in the next period)</td>
</tr>
<tr>
<td><strong>GVM.1.BP4: Ensure sharing of common vision.</strong> Ensure that individuals in the enterprise share a common culture, understand the common vision, and are committed and empowered to perform their functions effectively.</td>
<td>Coverage of key positions by governance policies and directives (e.g. rate of job descriptions related to implementing 11 governance objectives in payroll service)</td>
<td>Coverage of key positions by funding policies (e.g. rate of remuneration and bonus program expenditures in operating cash flow of payroll service)</td>
</tr>
<tr>
<td><strong>GVM.1.BP5: Establish and Maintain Strategy.</strong> 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</td>
<td>Coverage of business operations by specific business objectives (e.g. all business operation has customized business</td>
<td>Maintenance frequency of funding resource plans per business operations (e.g. funding resource plans are maintained quarterly for</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Application Practices for Competitiveness Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>be accomplished.</td>
<td>and governance objectives.)</td>
<td>payroll operation)</td>
</tr>
<tr>
<td>GVM.1.BP6: Formulate and align enterprise budgets. Formulate enterprise budgets to ensure alignment with strategic goals. Ensure congruency with action plans.</td>
<td>Maintenance frequency of budget plans per business operations (e.g. monthly in payroll service)</td>
<td>Maintenance frequency of cash flow plans per business operations (e.g. monthly in payroll service)</td>
</tr>
<tr>
<td>GVM.1.BP7: Develop and Deploy Action Plans. Establish, integrate, and deploy tactical action plans to accomplish strategic objectives.</td>
<td>Number of action plans per business operations in planning and reporting time horizons (e.g. one per business operations)</td>
<td>Specific funding plans per business operations in planning and reporting time horizons (e.g. funding for IT procurement in payroll service in the next year)</td>
</tr>
<tr>
<td>GVM.1.BP8: Review Performance. Review performance relative to goals and changing needs across the enterprise.</td>
<td>Performance review frequency per business operations (e.g. monthly in payroll service)</td>
<td>Efficiency review frequency per business operations (e.g. monthly in payroll service)</td>
</tr>
<tr>
<td>GVM.1.BP9: Act on Results of Review. Translate performance review findings into action.</td>
<td>Number of corrective action plans per business operations in planning and reporting time horizons (e.g. one in 3 month period in payroll service)</td>
<td>Unexpected funding requests per business operations in planning and reporting time horizons (e.g. extraordinary funding request for IT procurement in payroll service)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of CSR plan by business operations in planning and reporting time horizons (e.g. number of CSR programs related to payroll service)</td>
<td>CSR related funding plans per business operations in planning and reporting time horizons (e.g. financial resources for yearly CSR event of payroll service)</td>
</tr>
<tr>
<td>GVM.1.BP11: Inform employees regarding enterprise performance. Inform employees regarding enterprise performance.</td>
<td>Number of communications or events per business operations in planning and reporting time horizons (e.g. once per year in payroll service)</td>
<td>Communication expenditures per business operations in planning and reporting time horizons (e.g. funding for year-end celebration)</td>
</tr>
<tr>
<td>Evolve customer and other stakeholder needs and expectations. The organization applies</td>
<td>Coverage of revenue targets by service or</td>
<td>Availability of funding resources for service or</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Application Practices for Competitiveness Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>practices to elicit, analyze, clarify, and document evolving customer and other stakeholder needs and expectations.</td>
<td>product design works per business operations in planning and reporting time horizons aligned with strategy (e.g. 10% of revenue is resulted by implementation of new service elements)</td>
<td>product development per business operations in planning and reporting time horizons aligned with strategy (e.g. 10% of total funding is planned for development expenditures)</td>
</tr>
<tr>
<td><strong>LFC.1.BP1: Identify customers and stakeholders:</strong> Identify customers and stakeholders.</td>
<td>Revenue weights of identified customer and stakeholder types per business operations (e.g. ratio of different client categories by sector, size, activity, etc.)</td>
<td>Weights of different funding scenarios per business operations (e.g. specific payment options for service delivery, external funding requests, etc.)</td>
</tr>
<tr>
<td><strong>LFC.1.BP2: Elicit needs:</strong> Elicit customer and other stakeholders’ needs, expectations, and measures of effectiveness.</td>
<td>Number of identified customer and stakeholder needs per business operations (e.g. proposals for new service elements)</td>
<td>Number of identified funding requests for customer needs per business operations (e.g. funding request proposals for new service elements)</td>
</tr>
<tr>
<td><strong>LFC.1.BP3: Analyze needs:</strong> Analyze needs and expectations in the context of the intended operational environment.</td>
<td>Revenue weights of identified customer and stakeholder needs per business operations (e.g. ratio of different needs in sales)</td>
<td>Funding weights of customer needs per business operations (e.g. ratio of different needs in expenditures)</td>
</tr>
<tr>
<td><strong>LFC.1.BP4: Establish and maintain a statement of need:</strong> 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.</td>
<td>Number of formulized customer and stakeholder needs per business operations (e.g. new service elements)</td>
<td>Number of validated funding requests for customer needs per business operations (e.g. approved funding requests for new service elements)</td>
</tr>
<tr>
<td><strong>LFC.1.BP5: Communicate with customers:</strong> 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.</td>
<td>Number of communicated customer and stakeholder needs per business operations (e.g. new service portfolio elements)</td>
<td>Number of validated funding requests for communicated customer needs per business operations (e.g. approved funding requests of new service portfolio)</td>
</tr>
<tr>
<td><strong>LFC.1.BP6: Determine customer</strong></td>
<td>Coverage of revenue</td>
<td>Coverage of planned</td>
</tr>
</tbody>
</table>
### Application Practices for Competitiveness Governance Objective

<table>
<thead>
<tr>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets by customer satisfaction determination per business operations (e.g. there is only 50% coverage of revenue targets by determination of customer satisfaction)</td>
<td>expenditures by customer satisfaction determination per business operations (e.g. there is only 50% coverage of planned expenditures by determination of customer satisfaction)</td>
</tr>
<tr>
<td>Coverage of revenue targets by proposal preparation per business operations in planning and reporting time horizons aligned with strategy (e.g. 80% of revenue is resulted by proposal preparation practices)</td>
<td>Availability of funding resources for proposal preparation per business operations in planning and reporting time horizons aligned with strategy (e.g. 5% of total funding is planned for sales activities)</td>
</tr>
<tr>
<td>Coverage of revenue targets by service or product types per business operations in planning and reporting time horizons aligned with strategy (e.g. 80% of revenue is covered by service portfolio)</td>
<td>Coverage of planned expenditures by service or product types per business operations (e.g. 70% coverage of planned expenditures by service portfolio)</td>
</tr>
<tr>
<td>Coverage of revenue targets by risk criteria per business operations (e.g. 80% percentage of revenue is covered by risk criteria)</td>
<td>Coverage of planned expenditures by risk criteria per business operations (e.g. 70% coverage of planned expenditures by service portfolio)</td>
</tr>
<tr>
<td>Coverage of revenue targets by new requests for proposals per business operations (e.g. 25% of revenue is coming from new requests for proposals)</td>
<td>Coverage of planned expenditures by new requests for proposals per business operations (e.g. 15% coverage of planned expenditures by new requests for proposals)</td>
</tr>
</tbody>
</table>

### 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.

- **GVM.7.BP1: Evaluate Organizational Skills, Services and Products.** Examine and document the organizational goals, service 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.
<table>
<thead>
<tr>
<th>Application Practices for Competitiveness Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>according to established criteria. Identify the logical contenders for the proposal and their advantages.</td>
<td>Coverage of revenue targets by scope of preliminary sales research per business operations (e.g. 15% of revenue is under the scope of preliminary sales research)</td>
<td>Planned percentage of expenditures for preliminary sales research per business operations (e.g. 2% of planned expenditures for preliminary sales research)</td>
</tr>
<tr>
<td>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.</td>
<td>Percentage of No Go decisions per business operations (e.g. 40% of calls for proposal)</td>
<td>Percentage of No Go decisions due to funding criteria per business operations (e.g. 15% of No Go decisions caused by missing funding criteria)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of revenue targets by scope of proposal preparation team per business operations (e.g. 15% of revenue is under the scope of proposal preparation team)</td>
<td>Planned percentage of expenditures for new proposal preparation per business operations (e.g. 2% of planned expenditures for new proposal preparation)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of revenue targets by scope of communication interface per business operations (e.g. 75% of revenue is under the scope of proposal preparation team)</td>
<td>Planned percentage of expenditures for communication interface per business operations (e.g. 1% of planned expenditures for communication interface)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of revenue targets by scope of cost and resource estimates per business operations (e.g. 55% of revenue target is under the scope of cost and resource estimates)</td>
<td>Planned percentage of expenditures for cost and resource estimates per business operations (e.g. 2% of planned expenditures for cost and resource estimates)</td>
</tr>
<tr>
<td>GVM.7.BP8: Perform Estimation. Estimate costs and resources needed to satisfy the request.</td>
<td>Percentage of submitted proposals</td>
<td>Percentage of non-submitted proposals due</td>
</tr>
<tr>
<td>GVM.7.BP9: Prepare and Submit Proposal in Response to Acquirer Request. Prepare</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Application Practices for Competitiveness Governance Objective | Usefulness related metrics | Efficiency related metrics
--- | --- | ---
Proposal in accordance with guidelines in the acquirer’s request document or request | Per business operations (e.g. 40% of calls for proposal) | To lack of resources per business operations (e.g. 15% of proposals are not completed or submitted due to lack of resources)

GVM.7.BP10: Negotiate and Confirm Agreement. Negotiate relevant aspects of the agreement and formally confirm the agreement | Percentage of successful proposals per business operations (e.g. 40% of proposals) | Percentage of failed proposals due to funding problems per business operations (e.g. 15% of proposal are failed due to funding problems)

Table 19: Application Practices of Competitive Operation with possible metrics

The similarly established “Usefulness” and “Efficiency” metrics for the other (Control Management and Integrity Assurance) governance practices can help management to develop management assertions by selecting governance practices as risk criteria for the Strategic Business Goals.

By this way only those governance practices are scoped as capability indicators evidencing achievement of specific governance outcomes (Process Performance attribute), which are considered by the management as relevant based on its risk appetite. This consideration might be “instinctive” or even “conscious” by following the Managing Operational Risks scenario.

Managed capability (level 2) scoping takes reporting period based metrics into context of longer strategic planning periods, which allows performing trend analysis of historical data sourcing from multiple reporting data and periods.

Significant or dramatic (material) deviations from strategic plans indicate that internal or external risk factors should be reconsider followed by necessary actions in order to keep enterprise governance framework effective. This is why Managed capability - level 2 - scoping for governance processes is valid, as the wider/extended time-horizon and related objectives let management to use the performance metrics of the Managing Strategic Directions scenario as success or failure indicators of achieving longer term strategic business goals.

For example the trend for decreasing success rate of proposals may indicate lower competitiveness of the company jeopardizing business sustainability. However, handling only individual instances of deviations may take potential seasonal or unique reasons out of consideration.

Typically a governance process - as defined by the Governance Model for Trusted Businesses - is not performed as an individual project. For example Competitive Operation is incorporated into executive management of the company; Control Management and Integrity Assurance are under the direct supervision of the board. Therefore the Managed (level 2) capability of these governance processes is normally evidenced at executive and board level management, supervision and their supporting (e.g. sales, internal audit, etc.) activities.
4.6 Managing Operational Risks

4.6.1 Context and Specific Learning Objectives of Managing Operational Risks

The following figure presents role of the Managing Operational Risks scenario in supporting of Enterprise Governance:

![Role of the Managing Operational Risks scenario in Enterprise Governance](image)

Figure 18: Role of the Managing Operational Risks scenario in Enterprise Governance

In the context of Managing Operational Risks, Enterprise Governance should focus on those issues which are considered as relevant for the following sample management problems:

1. My company, which is well established and recognized by the target market, is running effective business operation(s) according to the stakeholder needs and expectations of the business environment; however increasing uncertainties - related to the market needs, the competitors, the technologies, the labour market, the regulatory environment and the funding conditions, etc. - request to implement a more robust risk management system.

2. We have several compliance audit reports (for financial controls, quality assurance, technical and environmental requirements, etc.); however they are not providing convincing evidences in assurance of achieving our business targets and avoiding failures.

3. We would like to measure effectiveness of our compliance, internal control and audit functions and efforts by their contribution to business success.

4. Stakeholders request more transparency over risk management and control of business operations.
5. We would like to qualify our business operations as according to the Governance Model for Trusted Businesses by presenting implementation of the governance processes in measurable and comparable forms.

Normally these issues are occurring and being managed in different time-scale than of the other Integrated Assurance Management scenarios. Managing Operational Performance is limited to the individual instances of the business processes and activities by considering service or product delivery requirements and schedule. Managing Performance Reliability considers contractual pay-off cycles with parallel or reoccurring business operational cycles, while Managing Operational Effectiveness typically has the time-horizon of the budgeting or reporting periods. Managing Strategic Directions is focusing on longer perspectives. Operational Risk Management takes each governance objective into its specific time-horizon when setting risk criteria and measurable risk levels for selecting treatment options and evaluating their effectiveness.

As presented at the other four Integrated Assurance Management scenarios, the reoccurring deviations from operational and organizational level Enterprise Goals call the management’s attention to check whether lower level governance objectives are adequately fulfilled. Lower level performance gaps might indicate longer term and higher level consequences, so they play early signaling role for management and supervision bodies. In case of no root cause having been found at lower levels then the governance objectives and related practices at the level where the deviation is identified should be carefully investigated.

The governance objectives are mediators between business goals and operational and organizational capabilities by keeping management directions aligned with the expectations of the stakeholders and the business environment. Therefore boards and other supervision bodies should be aware of and competent in how the overarching governance structure of the business entity is in compliance with the stakeholders needs. The Managing Operational Risks scenario provides the tools for overseeing operational and organizational management levels. Direct benefits of effective risk management are often not appearing in business success indicators, and mitigating controls or risk sharing methods might take significant efforts and costs. However risk management should make balance between costs and rewards for the overall benefit of the business stakeholders. Risk Awareness and Control Efficiency governance objectives and related governance practices together with Quantitative Performance Management are used to drive all the Enterprise Goals driven Integrated Assurance Management scenarios by adequately setting risk appetite and risk tolerances as risk criteria for measuring effectiveness of the more or less formulized risk treatment cycles performed by management activities.

Management actions taken to achieve governance objectives by implementing the Integrated Assurance Management scenarios under risk treatment cycles should be monitored by the board or other supervisory bodies (or by equivalent functions of the entity), and adequate level of transparency to all of the stakeholders should be provided by management disclosures.

This part of the case study material is focusing on the Managing Operational Risks scenario, which supports the achievement of strategic, operational effectiveness, reliability and performance objectives.

By the support of this Integrated Assurance Management scenario, the organization is enabled:

- 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;

- to ensure efficient usage of control resources relevant to the objectives of financial reporting and trusted business operation;

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
• to ensure that performance of the organization’s implemented governance processes support the achievement of the organization’s relevant business goals.

The enabling governance processes are:

• Control Risks, adapting practices from COSO
• Control Efficiency, adapting practices from COSO
• Quantitative Performance Management, adapting practices from ISO/IEC TR 15504-7

Applicable measures:

• Governance Capability - Risk Appetite (“usefulness”)
  - Indicator: specific and generic practices for governance processes
  - Time-horizon: as of related Integrated Assurance Management scenarios
• Alignment to Enterprise Goals - Risk Tolerance (“efficiency”)
  - Indicator: variance from established limits of Enterprise Goals
  - Time-horizon: as of related Integrated Assurance Management scenarios

In this part of the case study related to Managing Operational Risks scenario, the Risk Awareness and Control Efficiency governance objectives together with the Quantitative Performance Management practices are selected to provide applicable use cases for the following learning objectives:

• Which key risk and risk factors are mitigated by the governance objectives referred by
  o The Control Risks application area aiming 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.
  o The Control Efficiency application area aiming to ensure efficient usage of control resources relevant to the objectives of financial reporting and trusted business operation.
  o The Quantitative Performance Management application area aiming to establish and maintain a quantitative understanding of the performance of the organization’s processes through measurement and the use of appropriate quantitative techniques to ensure that performance of the organization’s implemented processes support the achievement of the organization’s relevant business goals.

• How to implement and evaluate application practices evidencing achievement of Risk Awareness governance objective through the following outcomes:
  o Governance objectives relevant for financial reporting and trusted business operation are established.
  o Risk assessments are performed consistently.
  o Organization’s internal controls are integrated with risks to achievement of organization’s objectives relevant for financial reporting and trusted business operation.
• How to implement and evaluate application practices evidencing achievement of **Control Efficiency** governance objective through the following outcomes:
  
  o *Adequate organizational structure and reporting lines are maintained.*
  
  o *Oversight of internal controls is effective.*
  
  o *Control deficiencies are reviewed and necessary actions are taken.*

• How to implement and evaluate application practices evidencing achievement of **Quantitative Performance Management** objective through the following outcomes:
  
  o *Processes or process elements are selected for quantitative management on the basis of their relevance and significance to the achievement of business goals;*
  
  o *Measures and analytical techniques to be used in statistically managing the processes or process elements are established and maintained;*
  
  o *Process performance data is collected and analyzed using appropriate statistical or other quantitative techniques to establish an understanding of the variation of the selected processes or process elements;*
  
  o *Results of data analysis are used to identify special causes of variation (assignable causes) in process performance;*
  
  o *Corrective and preventive actions are implemented to address the special and other causes of variation; and*
  
  o *Performance of the selected processes or process elements is monitored and controlled to establish stable, capable and predictable processes within control limits.*
4.6.2 Selecting the Scope of the Management Assertions for Managing Operational Risks

A consistent risk assessment should be performed as the first step to establish management assertions by linking business activities to applicable governance practices and capability profiles for supporting the relevant governance objectives.

By using the definition of risk as “effect of uncertainties on objectives”, during the Managing Operational Risks scenario we have to identify the risk criteria (tolerances and appetite) for not only those governance objectives which are enabling Risk Management, but also for all the others which are related to the other 4 Integrated Assurance Management scenarios as being under the scope of the Operational Risk Management. In terms of risk management related governance objectives we use the “Usefulness” and “Efficiency” measures for setting metrics in the specific time-horizons of the Integrated Assurance Management scenarios under the scope of risk management, for example:

- Risk Appetite measured by capability levels of governance processes enabling Integrated Assurance Management scenarios
- Risk Tolerance measured by variance from Enterprise Goals used by the Integrated Assurance Management scenarios.

For ensuring risk optimisation we need targets and tolerances e.g. measured by:

- Capability attribute ratings of governance processes (capability profiles), and
- Control limits of Enterprise Goals within the specific time-horizons of the Integrated Assurance Management scenarios.

The risk management related Risk Awareness and Control Efficiency governance objectives should also have such risk criteria which are applicable to measure effective risk treatment for achieving business goals and funding resources by applying governance practices. However these business goals and funding requirements are derived from those which have been used by the other Integrated Assurance Management scenarios. Applicable risk management related governance practices should be selected and implemented by considering their relevance to the above “Usefulness” and “Efficiency” measures.

If a lower level governance practice offered by the Governance Model has no significant relevance for the established operational and business unit/entity level Enterprise Goals, then there will be no need to apply that. If management specifies a governance practice as relevant for managing risks related to Enterprise Goals applied by the Integrated Assurance Management scenarios, then the target capability level for implementing this governance process will include it and will be also used as risk criteria (risk appetite). Capability level targets should be set aligned with all Integrated Assurance Management scenarios supporting achievement of their relevant Enterprise Goals.

Principles of Enterprise Risk Management are similar in each type of business organization. However related governance practices and their capability levels might differ in wide range. Effective small enterprises might run their business operation without extensive implementation of risk management practices. When business environment is changing, then the need for more formal and robust risk management will emerge. Managing risks is a challenge even for the more matured enterprises. By using of the Managing Operational Risks Integrated Assurance Management scenario, the management will be able to select and apply those governance practices which are relevant for improving overall enterprise governance.

Risk Awareness and Control Efficiency objectives related governance practices together with Quantitative Performance Measurement contribute to develop - level 4 - Predictable capability of those...
management processes which constitute management of business operation by establishing their organizational contexts.

Selection and implementation of those governance practices which are offered by the Governance Model for Trusted Businesses for Risk Awareness and Control Efficiency objectives should be driven by the management’s usefulness and efficiency considerations. Therefore the optimal (meaningful) coverage of offered governance practices, together with a capability profile aiming higher (e.g. Level 2 - Managed or Level 3 - Established) requirements should be concluded by performing mature risk management practices.

For supporting risk assessment the following risk tables for the Risk Awareness and Control Efficiency objectives can be used to understand key risk areas and applicable practices as risk responses:

<table>
<thead>
<tr>
<th>Key Risk</th>
<th>Risk Factors</th>
<th>Responses</th>
<th>Applicable COSO processes</th>
<th>Application Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance objectives for business processes are inadequately established</td>
<td>Management sets clearly defined objectives for governance including risk tolerance and risk appetite</td>
<td>Governance (Financial Reporting) Objectives (COSO)</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Inconsistency in risk assessment</td>
<td>Risk assessments are periodically performed by considering the time horizon of the governance objectives, risk tolerance and risk appetite</td>
<td>Governance (Financial Reporting) Risks (COSO)</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Risks relevant for organizations’ internal control system are not addressed</td>
<td>Control activities developed by reflecting to all assertions relevant for organization’s internal control system</td>
<td>Integration with Risk Assessment (COSO)</td>
<td>Actions are taken to address risks to the achievement of governance objectives relevant for financial reporting and trusted business operation.</td>
<td></td>
</tr>
</tbody>
</table>

Table 20: Risk Awareness related risk areas

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
How the governance objectives related risks are considered generally presents the risk culture of the organization. Through implementation of the Integrated Assurance Management scenarios - as presented in the previous chapters of this case study handbook - the governance objectives are customized in contexts and time-horizons of operational and organizational level Enterprise Goals. The target capability profiles of the governance processes being enabled by the selected specific and generic practices constitute the risk appetite for achieving these goals within established control limits (risk tolerances). For setting meaningful risk tolerances as control limits the Quantitative Performance Measurement process should be applied for indicating usefulness and efficiency measures used by the management assertions which present the linkage between business activities and governance practices. As the governance practices generally have wider scope than just mitigating downside of risks (as of the control activities), Quantitative Performance Management also supports to identify benefits from exploitation of business opportunities.

The implemented governance practices are tools for improving ability of the company to determine adequate risk appetite. Using of target governance capability profiles as risk appetite and quantitative control limits around Enterprise Goals as risk tolerances compose risk criteria applied by the risk treatment cycles (over Integrated Assurance Management scenarios) to measure residual status of risks. The selected governance practices provide implementation instances of the Control Risks governance process enabling the achievement of the following outcomes:

- Governance objectives relevant for financial reporting and trusted business operation are established.
- Risk assessments are performed consistently.
- Organization’s internal controls are integrated with risks to achievement of organization’s objectives relevant for financial reporting and trusted business operation.
Table 21: Control Efficiency related risk areas

By selecting and implementing Control Efficiency related governance practices for ensuring adequate governance (reporting and supervision) structure with sufficient management of reported control deficiencies for improvement, the risks and potential rewards should be compared to the increasing costs of improved controls (capability profiles) over business and governance processes. These considerations are applicable for all operational and organizational levels by following the Integrated Assurance Management scenarios.
Figure 19: Control Efficiency considerations in context of risk treatment costs

The selected governance practices provide implementation instances of the Control Efficiency governance process enabling the achievement of the following outcomes:

- Adequate organizational structure and reporting lines are maintained.
- Oversight of internal controls is effective.
- Control deficiencies are reviewed and necessary actions are taken.

The set of applied governance practices and the target Process Capability Attributes comprise those risk criteria against the business performance should be assessed. Evaluation of Process Attribute Gaps (between target and assessed capability) provides measurement of residual risk status.
4.6.3 Applying Management Assertions for Managing Operational Risks

Management assertions are setting links between the business processes (and activities) and the governance objective-driven processes (and base practices) offered by recognized reference models (like COSO, COBIT and Enterprise SPICE). Management should reflect to their own business goals and business environment’s expectations by setting target capability profiles for the customized governance objectives (risk appetite) and adequate quantitative control limits of tolerable deviations from Enterprise Goals (risk tolerance).

**Governance Capability Assessment** (Governance SPICE) methodology provides measurement framework for targeting and assessing effectiveness of governance processes (defined by ISO/IEC 15504 compliant reference models) in achievement of governance objectives, however it should be carefully considered at the assessment scope definition, that a governance process might be implemented and applied by more than one business processes (and their instances) within a business operational unit.

For example in the case of **Risk Awareness** objective concerning to the Monthly Payroll Calculation business process, the management should determine the management and control activities necessary and sufficient to limit the negative consequences of the inherent business risks related to the missing or inadequately defined governance objectives, inconsistent risk assessment and management assertions for implementing internal controls. These organizational contexts of the specific process performance are enabled by fulfilling the Predictable - level 4 - capability requirements.

Theoretically the management should apply a measure for determining direct impact on specific business goals, however at business process level this measure can’t derived directly from “natural” business measures like income, profitability, stock listing rate, market-share, etc. This problem could be resolved by targeting application of governance practices by the business process activities. The more relevant governance practices are applied; the negative consequences are the more likely minimized.

However the adequate structure of performance measurement helps to navigate over applicable governance practices (see Figure 4: Linking Governance Objectives to Enterprise Goals & Measures). The governance practices are enabling achievement of Enterprise Goals, so measurement related to achievement of governance objectives should support in-time status information regarding overall business performance. Furthermore the lower level operational or organizational goals and metrics should be established as enabling indicators for the above governance level.

**Quantitative Performance Measurement** is not only used for setting and evaluating metrics of achieving operational and organizational level Enterprise Goals, but also for establishing links among these governance levels. As normally the different level Enterprise Goals and their control limits are not directly comparable due to altering time-horizons and measurement units (like an individual process performance delay or error rate cannot be comparable with a missing yearly revenue target) the applied analytical evaluation techniques should support effective monitoring over different operational and organizational levels and time scales.

For selecting and prioritizing governance practices offered by the reference models, the **Managing Operational Risks** scenario offers “Usefulness” and “Efficiency” aspects of business performance. In case of Payroll Service Operation and Business Processes, the alignment to effective risk management should enable to define and implement **Risk Appetite** (measured by capability levels of governance processes enabling Integrated Assurance Management scenarios) and **Risk Tolerance** (measured by variance from Enterprise Goals used by the Integrated Assurance Management scenarios).
These two types of metrics help to identify relevance and weight of applicable governance practices in supporting performance objectives. If lack or failure of a governance practice - by considering together with other existing governance practices - represents undesirable uncertainty on keeping “Usefulness” or “Efficiency” goals, then implementation or improvement of the practice will be an adequate risk treatment option. If the lack or failure of a governance practice has no significant effect on Enterprise Goals - by considering together with other existing governance practices – this practice will be out of the scope of implementation and assurance. Performance measurement is needed to establish the concerning risk criteria and tolerance levels triggering immediate or scheduled management actions.

For example: a failure (performance gap) of COSO IFC.CA.IIRA Integration with Risk Assessment practices for Risk Awareness governance objective in a company running payroll outsourcing service – with sharing responsibilities over user organizations’ internal control - causes undesirable uncertainty in achievement of addressing risks relevant for both user and service organizations’ internal control system. Failures in e.g. mapping controls to relevant risks might cause overlapping or missing risk treatment actions leading to unpredictable performance of business operation. In this case an identified performance gap at maintaining Integration with Risk Assessment controls triggers the management actions for process improvement related to the Risk Awareness governance objective. External requirements for the service organizations controls over payroll service - like SOC 1 and SOC 2 – emphasize the relevance and importance of maintaining Integration with Risk Assessment controls.

The operational and organizational level “Usefulness” and “Efficiency” metrics used by the Integrated Assurance Management scenarios should be assessed against company targets (or other reasonable benchmark) and measures over pre-established tolerances should also trigger the (re)assessment of the Integration with Risk Assessment governance practices. If the assessed performance gap is significant as effecting one or more Enterprise Goal targets by exceeding their tolerances, then improvement action should be planned and implemented by the management. If detected performance gaps were not affecting significantly the Strategic, Operational Effectiveness, Reliability or Operational Performance related Enterprise Goals of the company running payroll service, then either the triggering tolerances of lower level performance metrics might be reset or - more likely - other related governance practices should be also assessed. Relevance and weight of a governance practice should be considered as an enabler of the related governance objective (like maintaining Integration with Risk Assessment controls enables achievement of Risk Awareness objective supporting Enterprise Goals at all operational and organizational levels).

At corporate level the governance objectives related set of practices comprising ISO/IEC 15504 compliant governance processes - as defined by the Governance Model - are applicable for targeting and assessing them for even higher (e.g. level 2 or above) governance capability. However from the selected business process view, as in the case of Monthly Payroll Calculation, the assessment target is mostly limited to Compliance (1 - Performed) level, as this is the level where the application of specific process outcomes and practices are investigated.

Targeting the Managed (level 2) or even higher level for the governance processes is applicable in the case when capability target of the Managing Operational Risks scenario were pre-established accordingly (e.g. in compliance with strict regulatory requirements). The higher capability request for Managing Operational Risks should be determined by the risk oversight bodies and also takes other affected business units (e.g. not just the Payroll Service Unit, but others like the Sales, IT Development, etc. units) into the same capability level context.
4.6.4 Selecting specific application practices as risk criteria for Managing Operational Risks

For fully achieving Process Performance attribute, the following specific outcomes should be evidenced concerning to the governance processes supporting Operational Risk Management (e.g. Payroll Service):

- for Control Risks governance process:
  - Governance objectives relevant for financial reporting and trusted business operation are established.
  - Risk assessments are performed consistently.
  - Organization’s internal controls are integrated with risks to achievement of organization’s objectives relevant for financial reporting and trusted business operation.

- for Control Efficiency governance process:
  - Adequate organizational structure and reporting lines are maintained.
  - Oversight of internal controls is effective.
  - Control deficiencies are reviewed and necessary actions are taken.

- for Quantitative Performance Measurement process:
  - Processes or process elements are selected for quantitative management on the basis of their relevance and significance to the achievement of business goals;
  - Measures and analytical techniques to be used in statistically managing the processes or process elements are established and maintained;
  - Process performance data is collected and analyzed using appropriate statistical or other quantitative techniques to establish an understanding of the variation of the selected processes or process elements;
  - Results of data analysis are used to identify special causes of variation (assignable causes) in process performance;
  - Corrective and preventive actions are implemented to address the special and other causes of variation; and
  - Performance of the selected processes or process elements is monitored and controlled to establish stable, capable and predictable processes within control limits.

The applied Governance Model for Trusted Businesses offers recognized best practices supporting these outcomes, however not all of them are necessary in context of the specific Enterprise Goals of the organization. Management should select only those practices as assertions, which have evidential link to “Usefulness” and “Efficiency” goals at this operational level. For Managing Operational Risks of a Payroll Service Company these goals are: definition and implementation of risk appetite and keeping risk tolerances for the operational and organizational levels aimed by the Integrated Assurance Management scenarios.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
For careful consideration, management should set metrics like described in the following sample table. Where current metrics show significant deviation from management’s expectations (risk appetite), the related practice should be implemented or improved. Where current metrics are available and satisfactory to reasonable risk appetite, the application practice can be set for management assertion.

Next table shows sample metrics for application practices supporting **Risk Awareness** governance objective:

<table>
<thead>
<tr>
<th>Application Practices for Risk Awareness Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Establish governance objectives for financial reporting and trusted business operation.</strong> 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.</td>
<td>Coverage of governance objectives by capability profiles - risk appetite (e.g. Fully achieved level 1 target for all)</td>
<td>Coverage of governance objectives by Usefulness and Efficiency metrics (e.g. metrics established for all outcomes of related governance processes)</td>
</tr>
<tr>
<td><strong>IFC.RA.FRO.BP1 Identify Management assertions.</strong> 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.</td>
<td>Coverage of governance objectives by management assertions (e.g. management assertions established for all outcomes of related governance processes)</td>
<td>Coverage of management assertions by Usefulness and Efficiency metrics (e.g. metrics established for all management assertions)</td>
</tr>
<tr>
<td><strong>IFC.RA.FRO.BP2 Consider the Range of Assessment Activities.</strong> 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 reality in a useful form.</td>
<td>Coverage of business operation by governance objectives (e.g. only mainstream business processes covered excluding supporting processes)</td>
<td>Coverage of business operation by Usefulness and Efficiency metrics (e.g. only mainstream business processes covered excluding supporting processes)</td>
</tr>
<tr>
<td><strong>IFC.RA.FRO.BP3 Compare Governance Policies.</strong> 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</td>
<td>Coverage of governance objectives by comparison (e.g. only generally published principles, like Accountability and Commitment)</td>
<td>Coverage of Usefulness and Efficiency metrics by comparison (e.g. no available metrics for comparison)</td>
</tr>
</tbody>
</table>
## Application Practices for Risk Awareness Governance Objective

<table>
<thead>
<tr>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>management and summarized for board review.</td>
<td>Coverage of governance objectives by capability assessment (e.g. all Integrated Assurance Management scenarios evaluated quarterly)</td>
</tr>
</tbody>
</table>

### 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.

#### 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 organization’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.

---

*This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*
<table>
<thead>
<tr>
<th>Application Practices for Risk Awareness Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>stakeholder needs)</td>
<td></td>
</tr>
</tbody>
</table>

**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.
- 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.

**Address risks relevant for financial reporting and trusted business operation.** Actions are

<table>
<thead>
<tr>
<th>Coverage of governance objectives by</th>
<th>Coverage of improvement/risk</th>
</tr>
</thead>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
### Application Practices for Risk Awareness Governance Objective

<table>
<thead>
<tr>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improvement/risk treatment actions per Integrated Assurance Management scenarios (e.g. improvement actions determined for all Integrated Assurance Management scenarios quarterly)</td>
<td>Treatment actions by referring to Usefulness and Efficiency metrics (e.g. metrics used as improvement indicators for all Integrated Assurance Management scenarios)</td>
</tr>
</tbody>
</table>

**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.

**Coverage of governance practices by improvement/risk treatment actions per governance objectives (e.g. improvement actions determined for all governance objectives quarterly)**

**Coverage of improvement/risk treatment actions per governance objectives by referring to Usefulness and Efficiency metrics (e.g. metrics used as improvement indicators for all governance practices implemented by the governance processes)**

**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.

**Frequency of workshops for evaluating effectiveness of improvement/risk treatment actions per governance objectives (e.g. improvement actions evaluated for all governance objectives quarterly)**

**Frequency of assessing residual risk impact by using Usefulness and Efficiency metrics (e.g. metrics used as effectiveness indicators for all governance practices implemented by the governance processes quarterly)**

**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.

**Coverage of governance processes and practices by mapping to evidences from business operation (e.g. full coverage of management assertions by using Stages Compliance Workbench)**

**Coverage of governance processes and practices by referring to Usefulness and Efficiency metrics (e.g. full coverage of management assertions by referring to metrics in Stages Compliance Workbench)**

**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.

**Coverage of governance processes and practices by mapping to evidences from business operation (e.g. coverage of management assertions)**

**Coverage of governance processes and practices by collecting Usefulness and Efficiency metrics (e.g. coverage of management assertions)**

---

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Table 22: Application Practices of Control Risks with possible metrics

Next table shows sample metrics for application practices supporting Control Efficiency governance objective:

<table>
<thead>
<tr>
<th>Application Practices for Risk Awareness Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFC.CA.IRA.BP5 Use independent assessment of outsourcing service provider’s internal control over processing transactions 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.</td>
<td>Coverage of outsourced business operation by assessing relevant governance objectives regularly (e.g. yearly assessment results are evaluated for Satisfaction, Accuracy and Data Protection)</td>
<td>Coverage of outsourced business operation by referring to Usefulness and Efficiency metrics for relevant governance objectives (e.g. metrics used as service level indicators for Satisfaction, Accuracy and Data Protection)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Practices for Control Efficiency Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure adequate organizational structure. The entity’s organizational structure supports effective internal control over financial reporting and trusted business operation.</td>
<td>Coverage of operational and organizational levels by governance objectives (e.g. Full coverage of key and supporting business processes in Payroll Service Unit and at enterprise level)</td>
<td>Coverage of operational and organizational levels by maintaining and using Usefulness and Efficiency metrics (e.g. metrics established and used by key and supporting business processes in Payroll Service Unit and at enterprise level)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of organizational levels by defined roles and reporting lines (e.g. Full coverage of key roles and reporting lines in Payroll Service Unit and</td>
<td>Coverage of organizational levels by defined roles for reporting and using Usefulness and Efficiency metrics (e.g. all roles and responsibilities defined)</td>
</tr>
<tr>
<td>Application Practices for Control Efficiency Governance Objective</td>
<td>Usefulness related metrics</td>
<td>Efficiency related metrics</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>IFC.CE.OS.BP2 Align Roles to Processes.</strong> Each unit or function within the organization aligns roles to key processes supporting governance objectives.</td>
<td>Coverage of operational levels by defined roles and reporting lines (e.g. Full coverage of key roles and reporting lines in Payroll Service operation)</td>
<td>Coverage of operational levels by defined roles for reporting and using Usefulness and Efficiency metrics (e.g. all roles and responsibilities defined for reporting and using metrics in Payroll Service operation)</td>
</tr>
<tr>
<td><strong>IFC.CE.OS.BP3 Maintain Job Descriptions.</strong> Management maintains job descriptions for key positions and updates them as conditions and circumstances warrant.</td>
<td>Coverage of operational and organizational levels by job descriptions (e.g. Full coverage of key and supporting business processes in Payroll Service Unit and at enterprise level)</td>
<td>Coverage of operational and organizational levels by job descriptions for reporting and using Usefulness and Efficiency metrics (e.g. job descriptions include responsibilities for reporting and using metrics of key and supporting business processes in Payroll Service Unit and at enterprise level)</td>
</tr>
<tr>
<td><strong>IFC.CE.OS.BP4 Establish Organizational Structures.</strong> 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.</td>
<td>Coverage of operational and organizational levels by Integrated Assurance Management scenarios (e.g. 5 Integrated Assurance Management scenarios covering Payroll Service operation)</td>
<td>Coverage of operational and organizational levels by Integrated Assurance Management scenarios using Usefulness and Efficiency metrics (e.g. 5 Integrated Assurance Management scenarios covering Payroll Service operation)</td>
</tr>
<tr>
<td><strong>IFC.CE.OS.BP5 Establish Structure for Internal Audit.</strong> An internal audit function reports directly to the Chief Executive Officer (CEO), with direct access to the oversight board (e.g. audit committee), to maintain independence over financial reporting and trusted business operation.</td>
<td>Coverage of operational and organizational levels by internal audit scope (e.g. audit scope of 5 Integrated Assurance Management scenarios covering Payroll Service)</td>
<td>Coverage of operational and organizational levels Usefulness and Efficiency metrics by internal audit scope (e.g. audit scope of 5 Integrated Assurance Management scenarios</td>
</tr>
<tr>
<td>Application Practices for Control Efficiency Governance Objective</td>
<td>Usefulness related metrics</td>
<td>Efficiency related metrics</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td><strong>Supervise internal controls.</strong> The oversight board understands and exercises oversight responsibility related to trusted business operation, financial reporting and related internal control.</td>
<td>Coverage of governance objectives by oversight board activities (e.g. all Integrated Assurance Management scenarios supervised quarterly)</td>
<td>Coverage of Usefulness and Efficiency metrics by oversight board activities (e.g. metrics used for supervision based on control limits for all Integrated Assurance Management scenarios)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP1 Establish Content for Board Meetings.</strong> 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.</td>
<td>Coverage of governance processes by meeting schedules (e.g. all identified gaps at governance processes, business units and supporting technology discussed quarterly)</td>
<td>Coverage of governance processes, business units and supporting technology by comparing capability gaps and trends of Usefulness and Efficiency metrics (e.g. supervision of all identified capability gaps compared to trends of related metrics)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP2 Identify Independent Board Members.</strong> Independent oversight board and/or audit committee members are identified.</td>
<td>Percentage of independent members in supervision of Integrated Assurance Management scenarios (e.g. 1/3 independent)</td>
<td>Percentage of independent members in supervision of Integrated Assurance Management scenarios (e.g. 1/3 independent)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP3 Establish Boards Roles and Responsibilities.</strong> The oversight board through the corporate bylaws, and the audit committee through its charter, set forth their roles and responsibilities.</td>
<td>Coverage of Integrated Assurance Management scenarios by oversight roles (e.g. dedicated board member for Risk Management oversight)</td>
<td>Coverage of quantitative performance measurement management by oversight roles (e.g. dedicated board member for quantitative performance measurement oversight)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP4 Consider Effectiveness of Internal Control.</strong> 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).</td>
<td>Frequency of meetings for evaluating effectiveness of improvement/risk treatment actions per governance objectives (e.g. improvement actions evaluated for all governance objectives)</td>
<td>Frequency of evaluating residual risk impact by using Usefulness and Efficiency metrics (e.g. metrics used as effectiveness indicators for all governance practices implemented by the governance)</td>
</tr>
<tr>
<td>Application Practices for Control Efficiency Governance Objective</td>
<td>Usefulness related metrics</td>
<td>Efficiency related metrics</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP5 Meet with Auditors.</strong> 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.</td>
<td>Frequency of meetings with auditors for maintaining capability targets (e.g. during evaluation of all Integrated Assurance Management scenarios quarterly)</td>
<td>Frequency of meeting with auditors for maintaining the Usefulness and Efficiency metrics per Integrated Assurance Management scenarios (e.g. control limits are reviewed by meetings for all Integrated Assurance Management scenarios quarterly)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP6 Review Policies and Procedures.</strong> The oversight board reviews governance policies and procedures used by management for determining significant expectations, including key assumptions.</td>
<td>Frequency of Risk Management reviews (e.g. during evaluation of all Integrated Assurance Management scenarios quarterly)</td>
<td>Frequency of reviewing the Usefulness and Efficiency metrics per Integrated Assurance Management scenarios (e.g. control limits are reviewed by meetings for all Integrated Assurance Management scenarios quarterly)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP7 Maintain Scepticism.</strong> 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.</td>
<td>Frequency of questioning management assertions per Integrated Assurance Management scenarios (e.g. quarterly)</td>
<td>Frequency of questioning control limits per Integrated Assurance Management scenarios (e.g. quarterly)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP8 Consider Whistle-blower Information.</strong> 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.</td>
<td>Frequency of Whistle-blower Information reviews (e.g. during evaluation of all Integrated Assurance Management scenarios quarterly)</td>
<td>Frequency of Whistle-blower Information reviews effecting the Usefulness and Efficiency metrics per Integrated Assurance Management scenarios (e.g. effect on control limits are reviewed by meetings for all Integrated Assurance Management scenarios quarterly)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP9 Review Board Candidates.</strong> The oversight board conducts due diligence on board and audit committee candidates to confirm appropriate</td>
<td>Coverage of governance objectives by competence certification/statements</td>
<td>Coverage of governance objectives by competence regarding quantitative</td>
</tr>
</tbody>
</table>

---

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Application Practices for Control Efficiency Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>independence from the organisation and management and his/her ability to be an effective board member.</td>
<td>(e.g. competence to Accountability objective)</td>
<td>performance measurement (e.g. competence of Accountability measurement)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP10 Certify Compliance.</strong> The oversight board members certify annually their compliance with the organisation’s ethics guidelines and independence rules.</td>
<td>Coverage of governance objectives by compliance certification/statements (e.g. compliance to Commitment objective)</td>
<td>Coverage of governance objectives by compliance certification/statements regarding quantitative performance measurement (e.g. competence of Commitment measurement)</td>
</tr>
<tr>
<td><strong>IFC.CE.OB.BP11 Meet with Management.</strong> 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.</td>
<td>Frequency of meetings without management per Integrated Assurance Management scenarios (e.g. during evaluation of all Integrated Assurance Management scenarios quarterly)</td>
<td>Frequency of meetings without managers for maintaining the Usefulness and Efficiency metrics per Integrated Assurance Management scenarios (e.g. control limits are reviewed by meetings for all Integrated Assurance Management scenarios quarterly)</td>
</tr>
<tr>
<td><strong>Manage internal control deficiencies.</strong> 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.</td>
<td>Number and frequency of improvement/risk treatment actions per Integrated Assurance Management scenarios (e.g. control improvement actions determined for all Integrated Assurance Management scenarios quarterly)</td>
<td>Coverage of improvement/risk treatment actions by using of Usefulness and Efficiency metrics (e.g. metrics used as effectiveness and efficiency indicators of control improvement actions for all Integrated Assurance Management scenarios)</td>
</tr>
<tr>
<td><strong>IFC.MO.RD.BP1 Report Information from Alternative Channels.</strong> Management establishes an alternative channel for reporting deficiencies sensitive in nature, such as illegal or improper acts.</td>
<td>Frequency of using information from alternative channels per Integrated Assurance Management scenarios (e.g. monthly review of information from alternative channels for all Integrated Assurance</td>
<td>Coverage of management reviews by considering of Usefulness and Efficiency metrics (e.g. metrics used by reviewing of information from alternative channels as measuring</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
**Table 23: Application Practices of Control Efficiency with possible metrics**

<table>
<thead>
<tr>
<th>Application Practices for Control Efficiency Governance Objective</th>
<th>Usefulness related metrics</th>
<th>Efficiency related metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IFC.MO.RD.BP2 Report Deficiencies to Various Levels in the Organisation.</strong></td>
<td>Management scenarios)</td>
<td>potential impact for all Integrated Assurance Management scenarios)</td>
</tr>
<tr>
<td>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.</td>
<td>Coverage of operational and organizational levels where deficiencies are systematically reported (e.g. deficiencies are reported by using of all Integrated Assurance Management scenarios)</td>
<td>Coverage of operational and organizational levels where control limits of Usefulness and Efficiency metrics are used for reporting deficiencies (e.g. deficiencies are systematically measured by using control limits of Usefulness and Efficiency metrics for all Integrated Assurance Management scenarios)</td>
</tr>
<tr>
<td><strong>IFC.MO.RD.BP3 Develop Guidelines for Reporting Deficiencies.</strong> 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.</td>
<td>Coverage of operational and organizational levels where guidelines of reporting deficiencies are established (e.g. guidelines of reporting deficiencies are maintained for using all Integrated Assurance Management scenarios)</td>
<td>Coverage of operational and organizational levels where guidelines of using control limits of Usefulness and Efficiency metrics are established for reporting deficiencies (e.g. guidelines of using metrics for reporting deficiencies are maintained for all Integrated Assurance Management scenarios)</td>
</tr>
</tbody>
</table>

The established “Usefulness” and “Efficiency” metrics for the Control Risks and Control Efficiency governance practices can help management to develop management assertions by selecting governance practices as risk criteria for the effective Operational Risk Management.

**Quantitative Performance Measurement** provides tools for the management to apply “Usefulness” and “Efficiency” metrics determined for all Integrated Assurance Management scenarios. Control limits of these metrics will drive necessary corrective and/or improvement actions enabling better achievement of Enterprise Goals. As all of the controls and other risk treatment actions should be considered in the context of Enterprise Goals, the “Usefulness” and “Efficiency” metrics related to governance practices have multiple functions. At first, they show residual risk status to be compared with established risk appetite, and at second, they establish links between governance objectives and Enterprise Goals by using control limits as risk tolerances. By applying the **Managing Operational Risks** scenario the capability level attribute ratings of the governance objectives related processes provide metrics for measuring risk tolerances in context of operational and organizational governance levels.
This observation is also valid for the **Risk Awareness** and **Control Efficiency** objectives. While management assertions determine applicable risk management practices as “reversed” risk appetite statements for operational risk management, the capability attribute ratings may be used as metrics for that. However, **Managing Operational Risks** scenario is different from the other 4 Integrated Assurance Management scenarios as also using target capability profiles related to all governance objectives for setting the tolerance levels around Enterprise Goal concerning Operational Risk Management.

By this way only those governance practices are scoped as capability indicators evidencing achievement of specific governance outcomes (Process Performance attribute), which are considered by the management as relevant based on its risk appetite. This consideration might be “instinctive” or even “conscious” by following the Managing Operational Risks scenario.

Managed capability (level 2) scoping takes metrics of altering time-horizons from different Integrated Assurance Management scenarios into the context of risk management planning. Risk evaluation and treatment cycles should follow the different characteristics of the covered Integrated Assurance Management scenarios, as applicable risk criteria are derived from the metrics of risk appetite (governance capability profiles) and risk tolerances (control limits for Enterprise Goals) within specific time-horizons.

Significant or dramatic (material) capability gaps or deviations out of control limits indicate that internal or external risk factors should be reconsidered followed by necessary actions in order to keep enterprise governance framework effective. This is why Managed capability - level 2 - scoping for governance processes is valid, as the wider/extended time-horizon and related objectives let management to use the performance metrics of the Managing Operational Risks scenario as success or failure indicators of achieving Enterprise Goals covered by the other Integrated Assurance Management scenarios.

For example the trend for not keeping control limits for important enterprise goals may indicate either that the related goals are not realistically established or the governance processes are not adequately implemented or maintained (for managing internal or external uncertainties affecting achievement of these goals). Managing Operational Risks scenario covering all the governance objectives may put those operational business processes into the organizational contexts of Predictable (level 4) process capability, which already “Fully achieved” the process attributes up to Established (level 3) capability by the support of the governance objectives related processes and practices covered by the other Integrated Assurance Management scenarios.

Typically a governance process - as defined by the **Governance Model for Trusted Businesses** - is not performed as an individual project. For example Control Risks governance process related practices are incorporated into risk or compliance management functions of the company; Control Efficiency governance process related practices are under the direct supervision of the board. Therefore the Managed (level 2) capability of these governance processes is normally evidenced at executive and board level supervision and their supporting (e.g. compliance, risk management, internal audit, etc.) activities.
4.7 Assurance Examples

4.7.1 Assurance on a Business Process at Managed level

The following example shows capability level 2 scoping for the Monthly Payroll Calculation business process presented in chapter 3.4.

As the management established its assertions concerning the Performance Goals by scoping on applicable business processes and Process Attributes up to Managed capability (level 2) the ISO/IEC 15504 conformant process assessment can be performed.

During assessment the evidences can be collected and presented by a process management platform like the Stages, and formal assessment can be performed and documented by the Capability Adviser tool.

The Enterprise Goals driven Integrated Assurance Management scenarios, like the Managing Operational Performance, may support that the assurance (process capability determination) and/or process improvement results of the assessment work provide real value for the organization, as helping better implementing and maintaining a customized enterprise governance framework.

The following assessment example presents defined business process activities for an on-going payroll service project and assessment statements for achieving Managed capability level targets by using Stages Compliance Workbench.

Assurance on Managed (level 2) capability of business processes in scope of operation helps management to identify improvement potentials over the business operation (like a contracted payroll service) level by focusing on better achievement of relevant performance goals. By applying Managing Operational Performance scenario the management should carefully consider the specific process activities and generic practices by using them as indicators (risk criteria) enabling better performance of the business operation.

<table>
<thead>
<tr>
<th>Name</th>
<th>%</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSM.MPC: Monthly Payroll Calculation</td>
<td>87.14</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management and performance of monthly payroll calculation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External: Payroll Cycle Management &amp; Supervision</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Table: Expenditure</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Table: Performance</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.PA1.1: Process Performance</td>
<td>83.57</td>
<td>Good</td>
</tr>
<tr>
<td>Custom rating</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outcomes evidenced by performance of the aligned business activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External: Performance of Monthly Payroll Calculation Process</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.BP1: Setting up and preparing for the payroll cycle</td>
<td>75.00</td>
<td>Good</td>
</tr>
<tr>
<td>Custom rating</td>
<td>75.00</td>
<td>Good</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Name</th>
<th>%</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rating justification</strong>&lt;br&gt;Coverage of volume and requirement changes per service elements: only 70% of changes were identical during preparation&lt;br&gt;Coverage of approved changes in capacity allocation for infrastructure, skills, material and human resources: only 80% of necessary changes in capacity allocation is admitted by the client</td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td>Assignments</td>
<td><strong>External: Preparation for Monthly Payroll</strong></td>
<td>80,00</td>
</tr>
<tr>
<td><strong>PSM.MPC.BP2: Collecting and recording clients' monthly payroll information based on agreed data-handling rules</strong></td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td><strong>Custom rating</strong></td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td><strong>Rating justification</strong>&lt;br&gt;Rate of exceptional cases per information types: 10% of employment data changes with missing formatting rules&lt;br&gt;Rate of overtime due to exceptional data takeover per staff category: 20% extra effort for manual data input by payroll clerk</td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td>Assignments</td>
<td><strong>External: Client's Data Takeover</strong></td>
<td>90,00</td>
</tr>
<tr>
<td><strong>PSM.MPC.BP3: Input data control and processing for payroll calculation with Client's control</strong></td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Custom rating</strong></td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Rating justification</strong>&lt;br&gt;Rate of non-processed data per input types: 20% timesheet data found inconsistent&lt;br&gt;Rate of overtime due to managing data errors per staff category: 20% extra effort for manual document checks and discussion by payroll clerk</td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td>Assignments</td>
<td><strong>External: Client's Control</strong></td>
<td>80,00</td>
</tr>
<tr>
<td><strong>External: Input Data Control and Processing</strong></td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td><strong>PSM.MPC.BP4: Checks and verifications of payroll calculation processing information</strong></td>
<td>75,00</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Custom rating</strong></td>
<td>75,00</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Rating justification</strong>&lt;br&gt;Coverage of requirements (check-list) per service elements: exceptional cases are double checked&lt;br&gt;Rate of actual to planned (allocated) verification effort: 100% extra verification effort due to exceptional cases</td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td>Assignments</td>
<td><strong>External: Process control and verification</strong></td>
<td>80,00</td>
</tr>
<tr>
<td><strong>PSM.MPC.BP5: Submission of all monthly payroll calculation outputs based on regulatory and agreed client's requirements</strong></td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td><strong>Custom rating</strong></td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td><strong>Rating justification</strong>&lt;br&gt;Rate of approval per service elements: accounting report rejected due to formatting error&lt;br&gt;Rate of extra output submission efforts and resources: 10% extra work due to manual report formatting</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Assignments</td>
<td><strong>External: Payroll Outputs Submission</strong></td>
<td>90,00</td>
</tr>
<tr>
<td><strong>PSM.MPC.BP6: Regulatory monthly reporting and documenting monthly payroll calculation process</strong></td>
<td>95,00</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
### BPM-GOSPEL

**Governance Capability Assessment**

**Case Study Handbook**

Integrated Assurance Management Scenarios for Trusted Business Operation

---

<table>
<thead>
<tr>
<th>Name</th>
<th>%</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom rating</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance rates of reporting/documentation elements: acceptance by tax authorities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate of extra reporting or documenting works: 10% more efforts for document filing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>External: Reporting and Documenting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSM.MPC.PA2.1: Performance Management</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generic Performance Management practices are evidenced by adapting Project Management governance practices in Payroll Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: Manage business project activities and resources</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.1.1: Identify the objectives for the performance of the process</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business activities are managed according to objectives established and maintained by the Payroll Service project plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 01. Define Project Objectives, Scope, and Outputs</td>
<td>100,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 02. Define the Life-Cycle Approach and Activities</td>
<td>100,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 03. Define Stakeholders</td>
<td>100,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.1.2: Plan and monitor the performance of the process to fulfil the identified objectives</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Activities are performed and monitored according to objectives established and maintained by the Payroll Service project plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 04. Estimate Planning Parameters</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 05. Estimate Project Resource Requirements</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 06. Establish Schedules</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 07. Establish Budget</td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 08. Plan the Quality</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 09. Develop the Human Resource Plan</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 10. Plan Communications</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 11. Plan Risks</td>
<td>75,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 12. Plan Procurements</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 13. Establish and Maintain Plans</td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 19. Monitor Project Performance</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.1.3: Adjust the performance of the process</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business activities are managed according to objectives established and maintained by the Payroll Service project plan.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
<table>
<thead>
<tr>
<th>Name</th>
<th>%</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 16. Direct and Manage Project Execution</td>
<td>100.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 20. Review and Analyze Project Performance</td>
<td>75.00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 21. Take Corrective Action</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.1.4: Define responsibilities and authorities for performing the process</td>
<td>95.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsibilities and authorities for business activities are established and maintained by the Payroll Service project plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 14. Establish Commitment</td>
<td>95.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 15. Acquire, Develop and Manage Project Team</td>
<td>95.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.1.5: Identify and make available resources to perform the process according to plan</td>
<td>95.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resources for business activities are identified and allocated according to objectives established and maintained by the Payroll Service project plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 06. Establish Schedules</td>
<td>95.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 12. Plan Procurements</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 17. Distribute Information</td>
<td>100.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.1.6: Manage the interfaces between involved parties</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication interfaces for business activities are identified and implemented according to the Payroll Service project plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 09. Develop the Human Resource Plan</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 18. Manage Stakeholder Expectations</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.PA2.2: Work Product Management</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generic Work Product Management practices are evidenced by adapting Project &amp; Quality Management governance practices in Payroll Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: Manage business project activities and resources</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: Provide quality management and assurance for business operation</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.2.1: Define requirements for the work products</td>
<td>95.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work products monthly payroll calculation are managed according to objectives established and maintained by the Payroll Service Manual.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 01. Define Project Objectives, Scope, and Outputs</td>
<td>95.00</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
### Table 24: Ratings of the Monthly Payroll Calculation process against - level 2 - Managed capability

<table>
<thead>
<tr>
<th>Name</th>
<th>%</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSM.MPC.GP2.2.2: Define the requirements for documentation and control of the work products</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Documentation and control procedures for work products related to monthly payroll calculation are established and maintained by the Payroll Service Manual.</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 08. Plan the Quality</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.2.3: Identify, document and control the work products</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Work products of monthly payroll calculation are identified, documented and controlled according to the Payroll Service Manual.</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 19. Monitor Project Performance</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 20. Review and Analyze Project Performance</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 21. Take Corrective Action</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>PSM.MPC.GP2.2.4: Review and adjust work products to meet the defined requirements</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Custom rating</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Work products of monthly payroll calculation are reviewed and adjusted according to the Payroll Service Manual.</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 3. Monitor Product and Service Quality</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 4. Monitor Noncompliance Issues</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 8. Monitor and Evaluate the Effect of Changes</td>
<td>95,00</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

By looking at the above example the following observations can be concluded:

1. If a business process is defined based on running well established business practice, then often the generic practices of Performance Management attributes will be naturally applicable and fulfilment of these criteria normally will not cause difficulties for the organization. However as formal definition of the process in context of specific operational performance represents less flexible requirements than they have been used in practice, some formal descriptions of required practices could be only evidenced with more implementation or improvement effort. Non-significant deficiencies from largely (over 85%) achievement of such practices should be carefully considered as potential sources of higher operational or organizational level weaknesses.

   For example “PSM.MPC.BP4: Checks and verifications of payroll calculation processing information” are routine tasks of the regular process performance, however the exceptional cases (like delay in processing schedule or extra manual data input or correction) may be out of scope of the formal verification practice, and documenting the control of these exceptional cases may be missed during process performance.

2. Sometimes it is difficult to distinguish performing controls as a base practice of a defined process and applying generic practices of - level 2 - Managed capability. Due to the ISO/IEC 15504 process definition requirement, that “no aspects of the measurement framework … beyond level 1 are contained or implied” by process outcomes, the base practices supporting achievement of these
outcomes should have other aspects than of the generic practices. Therefore fulfilling compliance type requirements and related practices should be targeted at level 1 process capability as process outcomes; however they can contribute to achievement of higher capability levels of other processes.

3. “Usefulness” and “Efficiency” metrics concerning process purpose and related base practices are tools for measuring both relevance and achievement of process goals. These measures can be interpreted as generic attributes, which might be valid at any capability level. For example similar measures might be also used at - level 4 - Predictable processes for process control, but in much wider organizational context than at level 1 capability. Using this metrics is an element of applying risk management cycles at each capability level.

4. The assessed high average rating (87.14%) for the level 1 and level 2 process attributes indicates that - with some limited improvement efforts - even the preconditions for targeting level 3 capability of the business process might be evidenced by this payroll service instance.

Assurance on Managed (level 2) capability helps management to identify improvement potentials over the business operation by focusing on better achievement of process performance goals. By applying Managing Operational Performance scenario the management should carefully consider the business processes and related control practices enabling better performance of the business operation in alignment with the operational level Enterprise Goals.

Applying Managing Operational Risks scenario will take these observations from assurance works into the context of risk management. The outcomes defined by the Monthly Payroll Calculation process together with the capability level target constitute the “reversed” form of risk appetite at the payroll project level. The “Usefulness” and “Efficiency” metrics regarding payroll calculation process performance serve as applicable risk tolerances. Risk treatment cycles include the setting of these risk criteria to measure the impact of the compliant or improved process performance driven by the risk treatment actions.
4.7.2 Assurance on a Governance Process

The following example shows capability level 1 scoping for **Satisfaction** governance objective related process. The sample scope setting is targeting Fully (more than 85%) achievement of **Process Performance** attribute of the related **Satisfactory Operation** process of the **Governance Model for Trusted Businesses** used as applicable Process Reference Model according to ISO/IEC 15504 (SPICE) measurement framework.

As the management established its assertions concerning the **Reliability Goals** by scoping on applicable governance practices and **Process Attributes** to **Performed** capability (level 1) the ISO/IEC 15504 conformant process assessment can be performed.

During assessment the evidences can be collected and presented by a process management platform like the **Stages**, and formal assessment can be performed and documented by the **Capability Adviser** tool.

The **Enterprise Goals** driven Integrated Assurance Management scenarios, like the **Managing Performance Reliability**, may support that the assurance (process capability determination) and/or process improvement results of the assessment work provide real value for the organization, as helping better implementing and maintaining a customized enterprise governance framework.

The following assessment example presents selected model based governance practices as management assertions for an on-going payroll service project and assessment statements for achieving **Performed** capability level targets for the **Satisfaction** objective related governance process from the **Governance Model for Trusted Businesses** by using Stages Compliance Workbench.

<table>
<thead>
<tr>
<th>Name</th>
<th>%</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOV.SOP: Satisfactory Operation</td>
<td>83.50</td>
<td>Good</td>
</tr>
<tr>
<td>Custom rating</td>
<td></td>
<td>85.00</td>
</tr>
<tr>
<td>Rating justification</td>
<td>Satisfactory Operation supports achievement of client retention and capacity utilization business objectives during pay-off period of investigated Payroll Service operation.</td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process: Monthly Payroll Calculation Process</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Process: Payroll Cycle Management &amp; Supervision</td>
<td>85.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Table: Client Satisfaction Index</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Table: Exceptional Work Index</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>GOV.SOP.PA1.1: Process Performance</td>
<td>82.00</td>
<td>Good</td>
</tr>
<tr>
<td>Custom rating</td>
<td></td>
<td>80.00</td>
</tr>
<tr>
<td>Rating justification</td>
<td>Outcomes evidenced by performance of the selected governance practices adapting Satisfactory Operation</td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: Adapting Satisfactory Operation</td>
<td>90.00</td>
<td>Excellent</td>
</tr>
<tr>
<td>External: Link to Evidences</td>
<td>50.00</td>
<td>Good</td>
</tr>
<tr>
<td>GOV.SOP.BP1: Establish and maintain requirements that meet customer needs and expectations</td>
<td>78.00</td>
<td>Good</td>
</tr>
<tr>
<td>Custom rating</td>
<td></td>
<td>78.00</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
**Table 25: Ratings of the Satisfactory Operation and its enabling Governance Practices**

<table>
<thead>
<tr>
<th>Name</th>
<th>%</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>elements have approved requirement specification</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage of approved capacity allocation for infrastructure, skills, material and human resources: only 75% of necessary capacity allocation is admitted by the client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 1. Identify Requirements</td>
<td>60,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 2. Derive Requirements</td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 3. Analyze Requirements</td>
<td>50,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 4. Baseline Requirements</td>
<td>40,00</td>
<td>Fair</td>
</tr>
<tr>
<td>Activity: 5. Analyze Requirements Risks</td>
<td>50,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 6. Manage Requirements Changes</td>
<td>40,00</td>
<td>Fair</td>
</tr>
<tr>
<td>Activity: 7. Ensure and Maintain Requirements Traceability across the Life Cycle</td>
<td>30,00</td>
<td>Fair</td>
</tr>
<tr>
<td><strong>GOV.SOP.BP2: Manage relationship among business stakeholders</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom rating</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage of relationship types: contracting, operational supervision and day-to-day contact levels defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allocated time and resources per relationship types: monthly half day meeting at customer’ site including operational manager and payroll clerk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 1. Develop Relationships</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 2. Establish Interactive Communication Methodologies and Structures with Stakeholders and Partners</td>
<td>80,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 3. Identify Relationship Attributes</td>
<td>50,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 4. Identity Value Creation Opportunities</td>
<td>75,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 5. Manage Complaints and Compliments</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 6. Create Service Level Agreements</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 7. Establish a Service Catalog</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td><strong>GOV.SOP.BP3: Operate according to agreed service levels</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom rating</td>
<td>85,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Rating justification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Satisfaction rate per pay-off period: 100% coverage of agreed service level in monthly payroll calculation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deviation (range) from planned resources: 15% staff overwork in monthly payroll calculation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity: 1. Operate the Product or Service</td>
<td>100,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 2. Establish Methods</td>
<td>60,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 3. Monitor and Evaluate Capacity, Service, and Performance</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 4. Confirm Availability of Resources</td>
<td>60,00</td>
<td>Good</td>
</tr>
<tr>
<td>Activity: 5. Perform Corrective and/or Preventive Maintenance</td>
<td>100,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 6. Analyze Failures</td>
<td>100,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 7. Take or Initiate Corrective Action</td>
<td>100,00</td>
<td>Excellent</td>
</tr>
<tr>
<td>Activity: 8. Provide Customer Support</td>
<td>90,00</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
By looking at the above example the following observations can be concluded:

1. Rating of a management assertion - assigned as an activity in Stages implementation - might have no direct impact on the related base or generic practice rating. As assertions are selected and prioritized as risk appetite (and if adequately measured then they will be used as risk criteria) to specific business objectives, there is no general rule that fulfilment of an individual model based best practice - assigned as an activity in Stages - is sufficient or necessary to achieve the level 1 or even higher capability outcomes of a governance process defined by the **Governance Model for Trusted Businesses**. However the rating value under 50% shows either that the concerning practice is not really relevant under the specific business conditions or that a significant improvement is needed. E.g. improvement of activities assigned as assertions to “GOV.SOP.BP1: Establish and maintain requirements that meet customer needs and expectations” would result over 85% (Largely) achievement of that base practice necessary for level 1 capability of **Satisfactory Operation**.

2. The base or specific practice ratings have effect on process attribute ratings. The gap to 85% at “GOV.SOP.BP1: Establish and maintain requirements that meet customer needs and expectations” practice causes also a gap to the fully (over 85%) achievement of the Process Performance level 1 attribute. The assessor also marked the customized rating of the process attribute to 80% (a lower level than the average of base practice ratings) as the presented (linked) evidences are not sufficient (rated as only 50%). Therefore aiming fully (over 85%) achievement of the Process Performance attribute will request both improvement of the lower rated base practice (e.g. by improvement of enabling practices assigned as activities) and better presentation of the identical evidences.

3. The high average rating (83,50%) for the level 1 process attribute indicates that - with some limited improvement efforts - even the preconditions for targeting higher capability levels of the **Satisfactory Operation** governance process at business unit level might be evidenced by this payroll service instance.

Assurance on Managed (level 2) capability of **Satisfaction, Accuracy and Data Protection** objectives related governance processes (of the **Governance Model for Trusted Businesses**) would help management to identify improvement potentials over the business operation (like a contracted payroll service) level by focusing on better achievement of relevant goals for customer retention and capacity utilization. By applying **Managing Performance Reliability** scenario the management should carefully consider the governance processes and practices enabling better performance of the business operation in alignment with the operational level Enterprise Goals.

As the example shows the improvement of requirements management and communication practices (having lower ratings in the above assessment profile) might lead to better customer satisfaction and efficiency in using resources, being realized by the payroll service operations during pay-off cycles. Managed (level 2) capability for the operational and the enabler processes would provide even higher level of assurance. The Integrated Assurance Management scenario provides tool for the management of getting the sufficient assurance level at reasonable implementation and audit efforts and costs by keeping in hand the necessary decisions over the governance framework.

Using processes from the Governance Model for Trusted Businesses is enhancing the process capability profiles of the business operation. The traditional applications of well recognized ISO/IEC 15504 (SPICE) models often have difficulties as over level 2 assessments - like assurance on Established (level 3) and Predictable (level 4) process capability - request different management scoping than of the individual or “project-level” instances of operational processes. Process attributes for level 3 and 4 are established on business unit/entity level objectives, which are not directly related to the process performance goals or outcomes as defined by the reference models.

At business unit or entity level the business processes are operating in special context of the organization and not just in context of the applied process assessment model. For keeping consistency and reliability of...
level 3 and level 4 capability profiles among organizations of different types, sizes, ownership structures, sectors, etc., the enterprise goals driven “enabler” processes can be used to better interpret ISO/IEC 15504 based generic process attributes and their assessment indicators.

For example the enabling governance processes used by the Managing Reliable Performance scenario provide organizational context to all operational business processes within the common scope, through setting and achievement of **Satisfaction, Accuracy and Data Protection** objectives being customized by the operational management. The - level 3 - Established (standardized and effectively deployed) payroll service process cannot be comparable among different service providers if its sequence and interaction with other processes were not based on common and understandable governance framework. This is the way of changing the traditional model based check-listing assurance works towards Enterprise Goals driven Risk Management.