TRUSTED BUSINESS

EU Project BPM-GOSPEL – Applying Compliance Management Scenarios in Business Process Modelling for Trusted Business Coaching Programs

BPM GOSPEL

(2010-1-HU1-LEO05-00036)

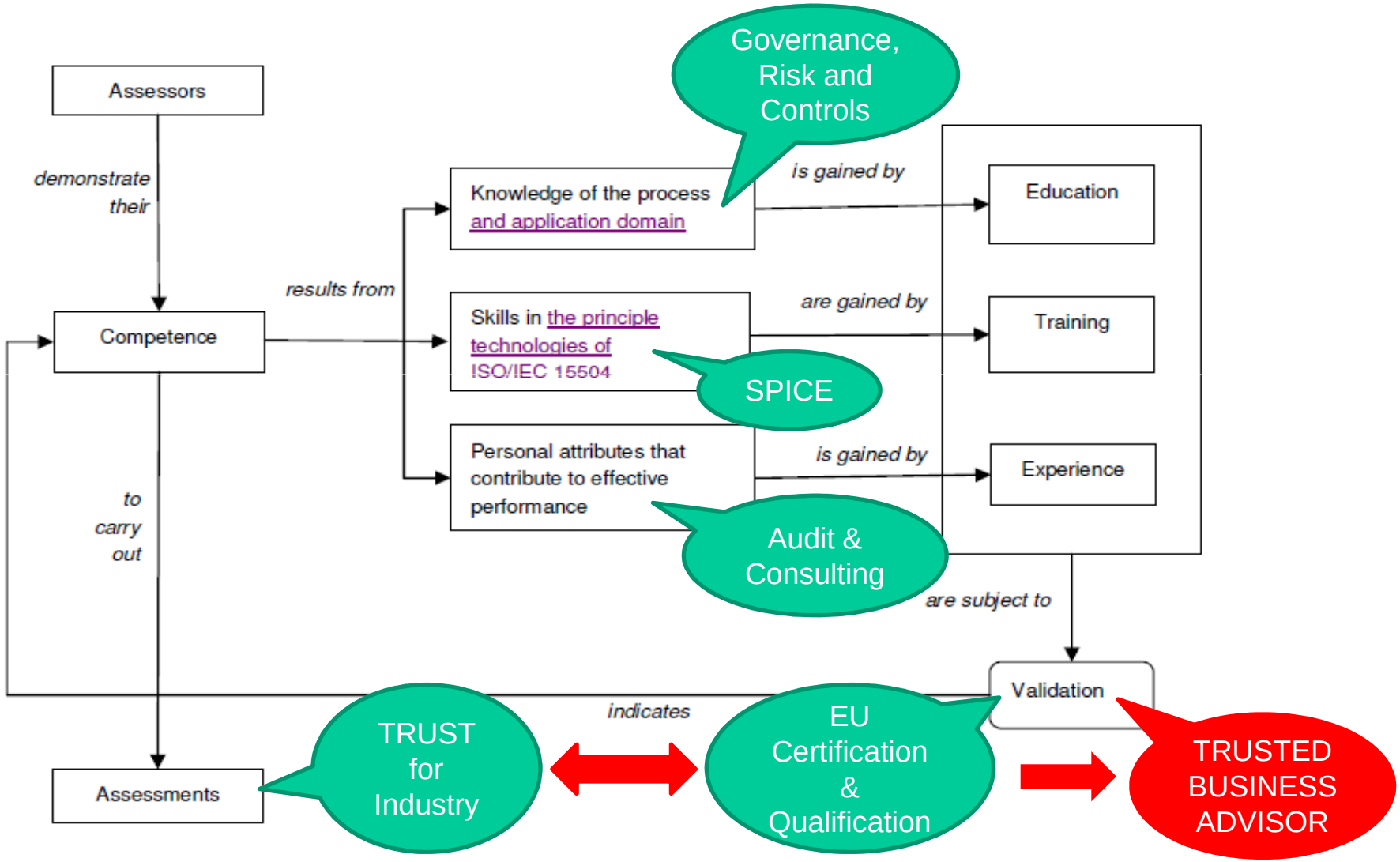
This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

19th EuroSPI Conference, BENA Business Base Nineteen, Vienna, Austria, 25.-27.06.2012

Topics

- Trust and Effective Enterprise Governance
- ”Governance” SPICE Roadmap (2005-2012)
- Using COSO, COBIT & ESPICE Process Reference Models
- Linking Governance to Sustainable Value Creation
  - Trusted Business Model and extension of ECQA certified Governance SPICE Assessor Skill Card
  - Multi-layer business assurance technology
- Certification and Qualification for Trusted Business
  - ECQA JRC activities
  - 2-level Qualification Scheme for Trusted Business
- From Compliance Management to Operational Risk Management
  - Linking Governance Objectives to Enterprise Goals & Measures

Validation of Governance SPICE Competencies



Why Industry Needs Trust?

Turbulent economic environment

- Financial crisis & economic downturn
- Global impact on local/sectoral markets
- General cost cutting leads to decline of available (in-house and/or outsourced) competency levels

Stakeholders' expectations

- Predictable business benefits (more explicit tolerance levels)
- Conservative risk-taking (redefinition of risk appetites)
- Higher management accountability (with balanced compensation)
- No governance scandals or regulatory non-compliance issues jeopardizing reputation
- Cost effective controls (less duplicates or overlaps)

Sector specific

- More interdependences among business partners
- Faster reaction on market needs
- Supply chain management requests long term credibility

How Trust Needs Effective Governance?

Less isolated risk & compliance management programs

- More responsibility of the ”Chief Executive” level management
- Set links between strategic business objectives and management control processes
- Integrated assessment/audit approaches

Transparency

- Applying business objectives for managing/supervising compliance programs
- Presenting excellence in an understandable way (format)
- Using competent and qualified human resources
- Assuring accuracy by harmonizing time horizons to business objectives

Coverage

- Defining the business operation boundary conditions
- Leveraging the business opportunities (sustainability)
- Addressing the sector-specific technical/regulatory (control) requirements of the core business activities

”Governance” SPICE Roadmap (2005-2012)

Refers to

- Governance, Risk and Controls (OECD Principles, Regulations, Audit Standards)

based on different concepts (IA-Manager 2005-2007)

- Recognized Control Frameworks (COSO&COBIT)
- Risk Tolerance and Risk Appetite (COSO ERM)
- Performance Measurement (COBIT)
- Process Capability Assessment (ISO/IEC 15504-2)
- Evaluating Process-related Risk (ISO/IEC 15504-4)
- Organizational Maturity (ISO/IEC TR 15504-7)

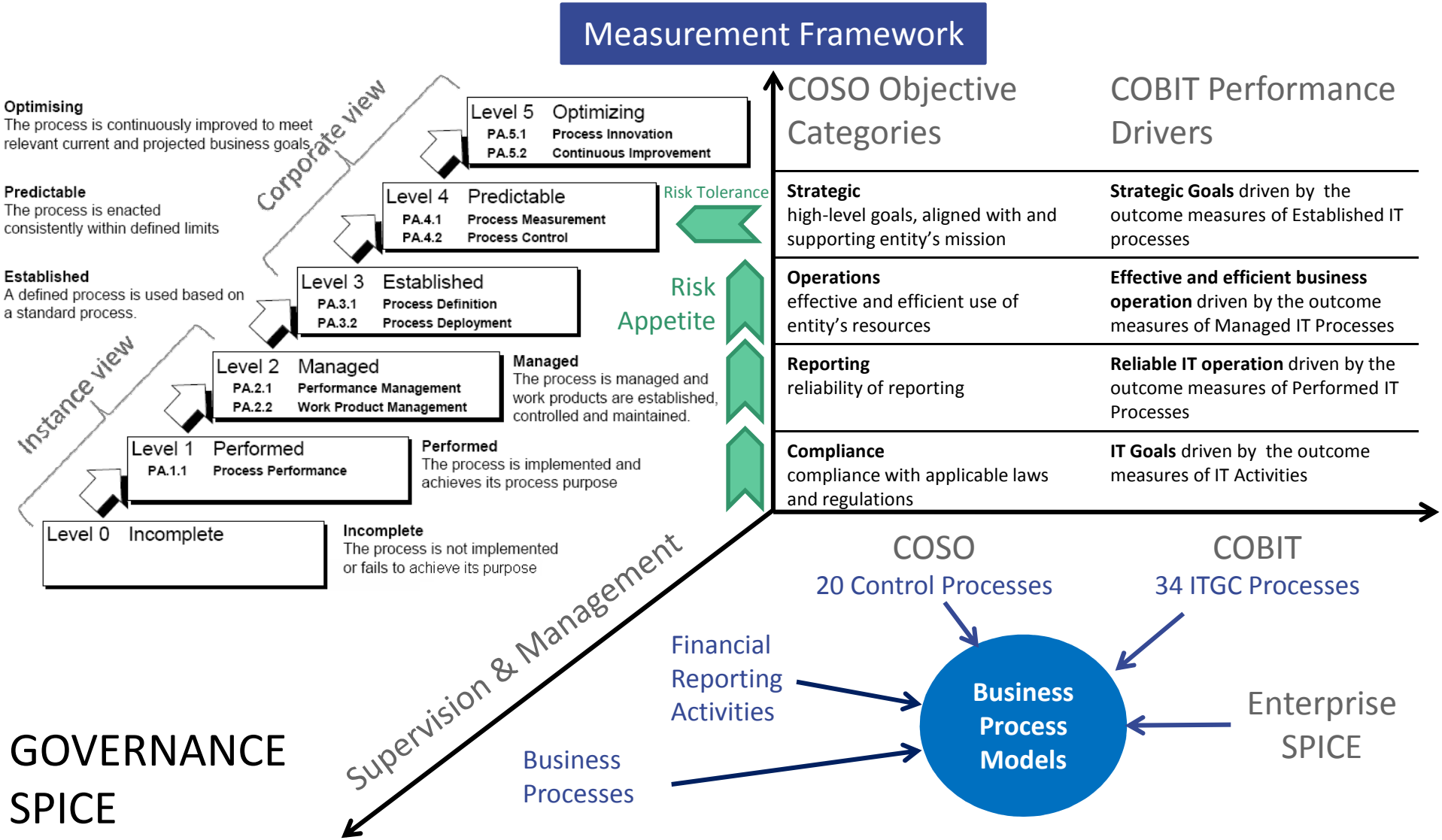
by using multilingual ontology (MONTIFIC 2008-2010)

- Terminology database
- Ontology model for training

to leverage sustainable value creation (GOSPEL 2010-2012)

- New ”Trusted Business Model” and extension of Governance SPICE Assessor Skill Card
- Multi-layer business assurance technology supporting coaching (assessor training) programs

Using COSO, COBIT, etc. Processes for Assessment



Why a new model is needed?

- The well established and recognized control frameworks and process reference models – like COSO and COBIT - could be used for effective and efficient enterprise governance, if only the management established its own governance related objectives.
- Unfortunately, structures of control frameworks and reference models are not easily interpretable by enterprise management for setting their business' specific governance objectives.
- Furthermore, the external and internal audit standards and literatures are also not really supportive in these terms.

Trusted Business Model

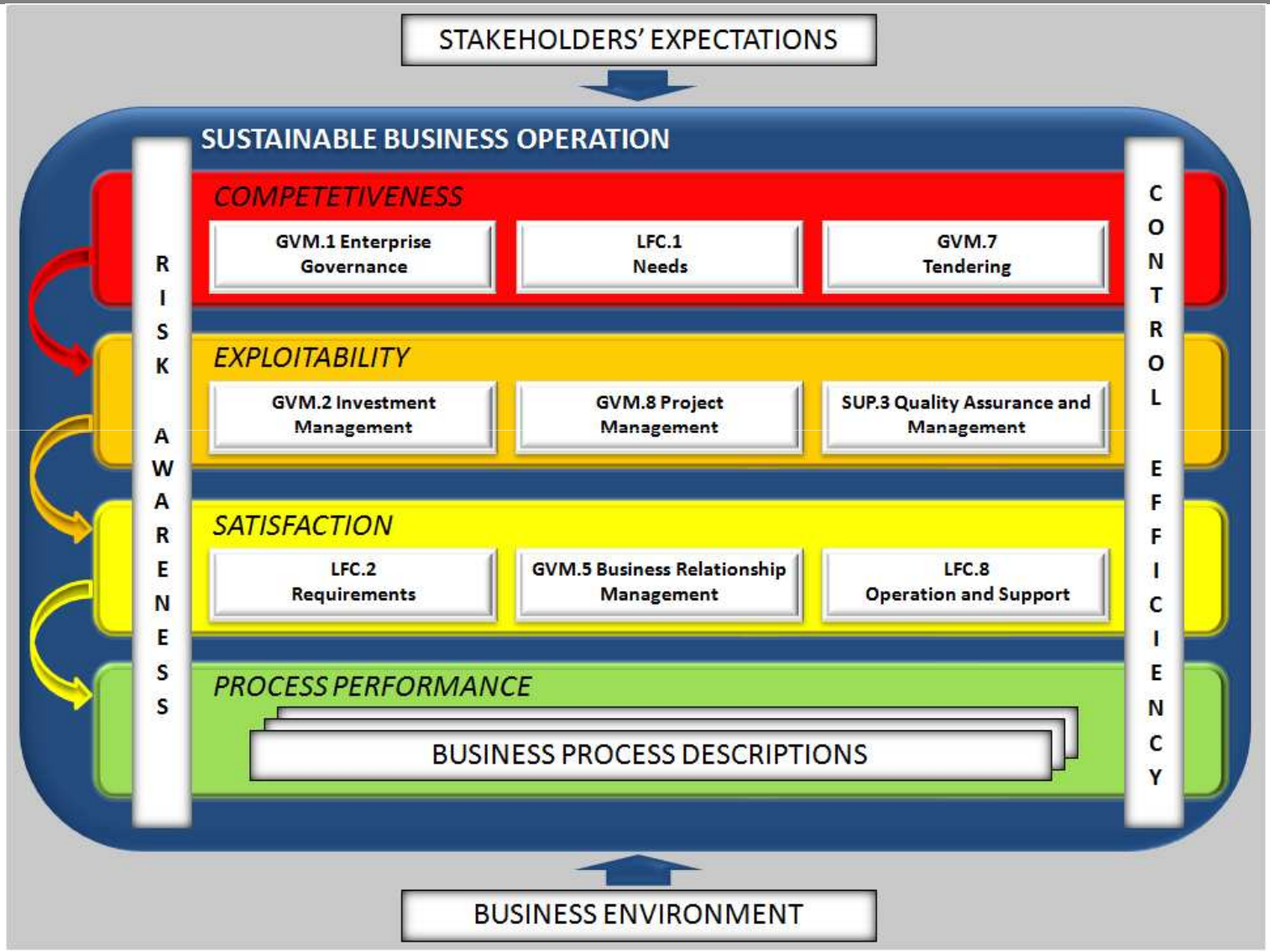
The new Model

- keeps both enterprise management and audit assurance logics in mind
- by presenting governance processes in line with the objectives relevant for enterprise management,
- together with an exact mapping to processes of control frameworks (reference models) accepted and used by auditors for compliance attestation.
- Provides descriptions and application practices of governance processes for management assertions and audit reports for providing assurance of trusted and sustainable business operation.

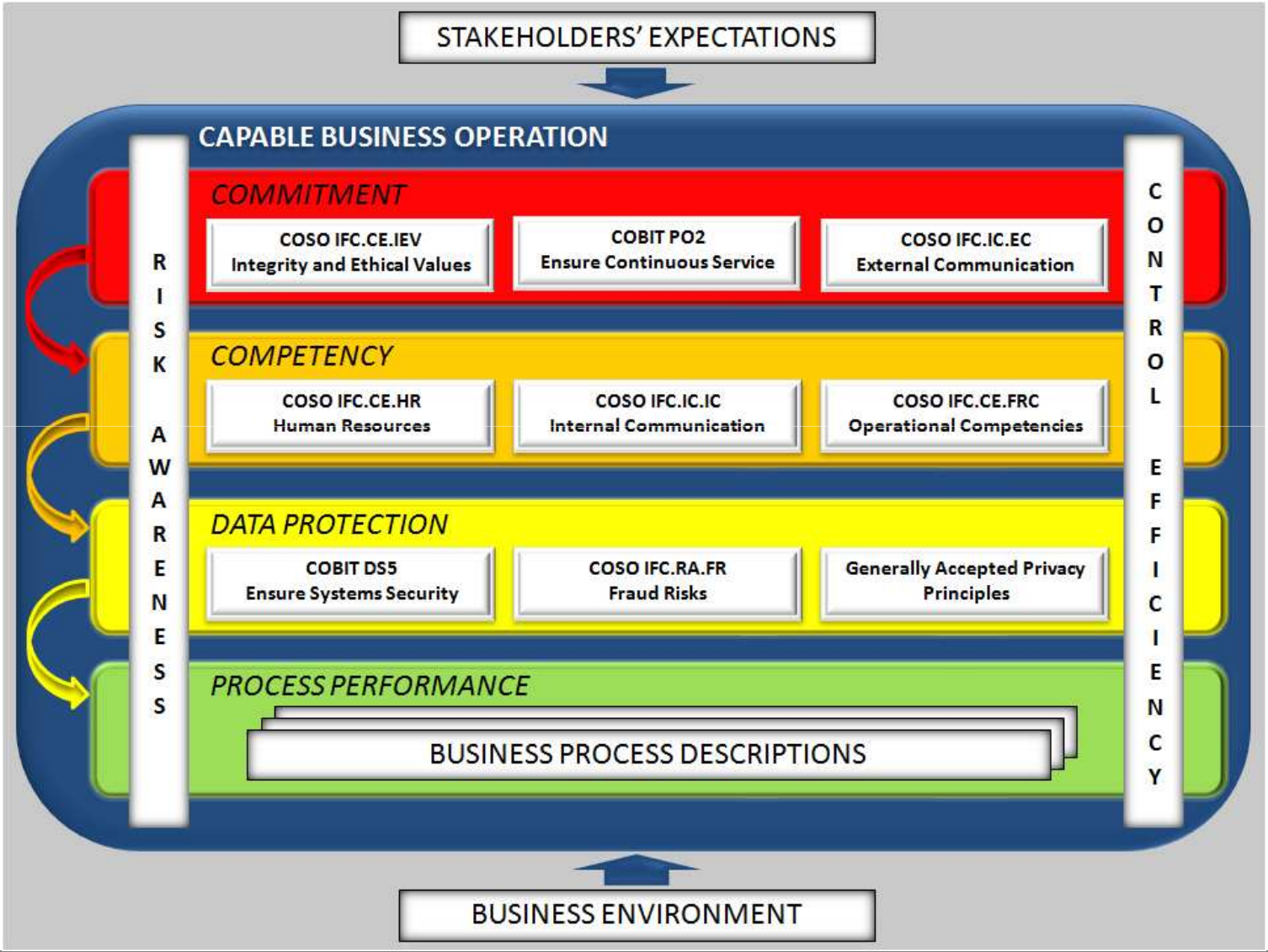
Trusted Business Model
Setting Governance Objectives

- Supporting Business Sustainability (leveraging opportunities)
  - Competitiveness (ESPICE)
  - Exploitability (ESPICE)
  - Satisfaction (ESPICE)
- Supporting Organization's Internal Control System
  - Risk Awareness (COSO)
  - Accountability (COSO)
  - Competency (COSO)
  - Accuracy (COBIT, COSO)
  - Process Integrity (COSO)
  - Data Protection (COBIT, COSO, GAPP)
  - Commitment (COBIT, COSO)
  - Control Efficiency (COSO)

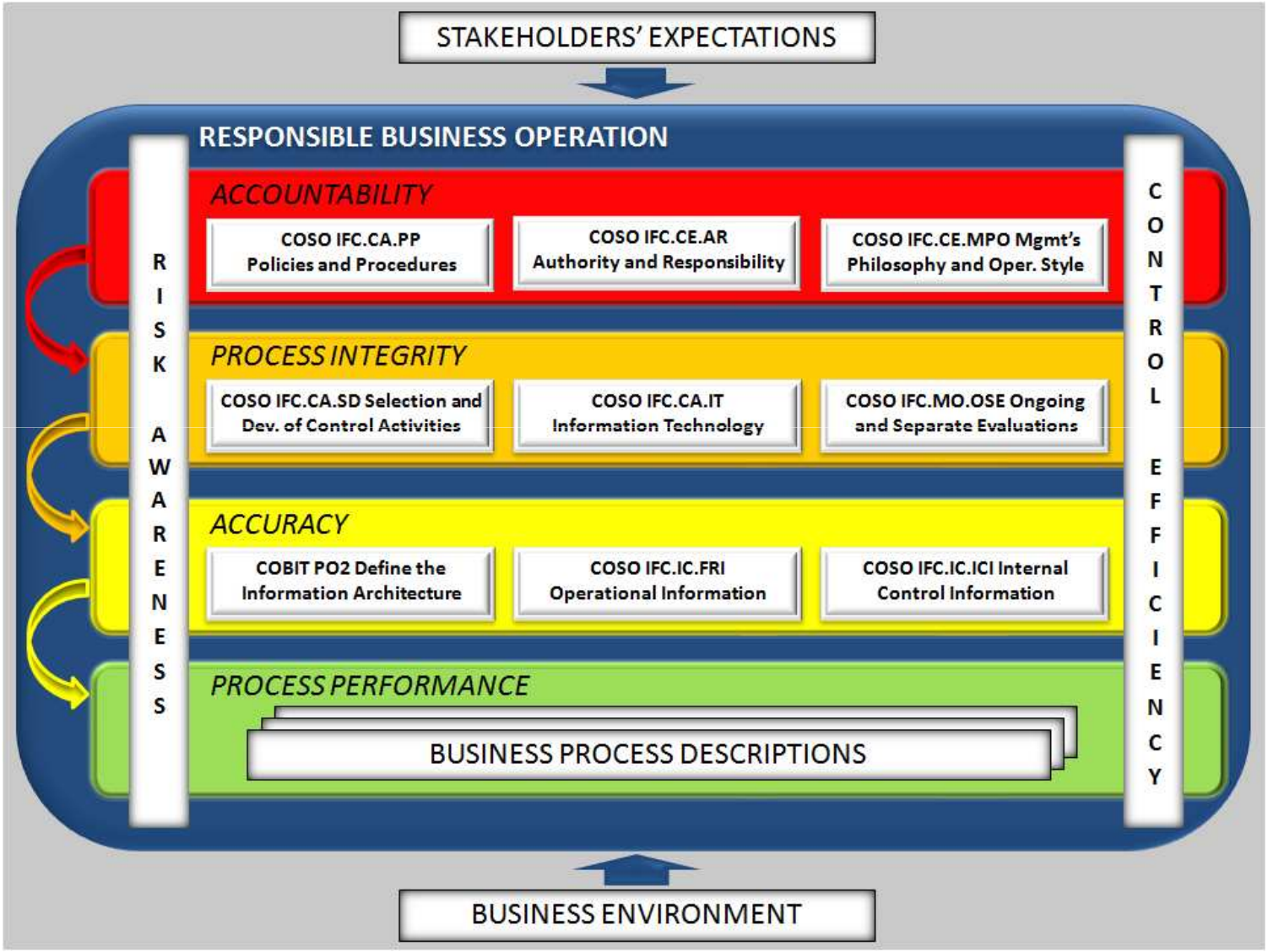
Mapping with Enterprise Goals 1. Sustainable Business Operation (ESPICE)



Mapping with Enterprise Goals 2. Capable Business Operation



Mapping with Enterprise Goals 3. Responsible Business Operation



Determining Application Process for a Governance Objective (Accuracy)

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

Information Reliability – Governance Process (Accuracy Objective)

Process ID	GOV.IR
Process Name	Information Reliability
Process Purpose	The purpose of the Information Reliability process is to ensure the accuracy and consistency in data architecture and disclosure elements relevant for financial reporting and trusted business objectives, and for supporting data processing integrity. NOTE1: The Information Reliability process is **a special application** of the COSO 2006 and COBIT 4.1 models in the context of the "**Accuracy**" governance objective. Thus this process is denoted an "Application Area". The practices, called "application practices", are implemented using selected processes based on the COSO 2006 principles and the COBIT 4.1 framework in the context of this special application. This facilitates the re-use of the elements of the COSO 2006 and COBIT 4.1 based reference models without recreating processes that are already well established. NOTE2: The descriptions of the COBIT 4.1 processes and the COSO 2006 Principles are applicable to define ISO/IEC 15504 conformant process reference models and process performance indicators for assessing process capability according to the ISO/IEC 15504 standard.
Process Outcomes	As a result of successful implementation of the Information Reliability process the following service governance objectives are achieved: 1) Effective information architecture and data model are maintained. 2) Information is systematically collected and assessed to detect compliance issues, privacy problems and fraud. 3) Control information for automated process settings, data manipulations and calculations are maintained systematically.

Using ”Define the Information Architecture” COBIT Process as an Application Practice

Application practice	**AP01 Ensure the integrity and consistency of all data stored in electronic form.** Satisfy the business requirement of being agile in responding to requirements; provide reliable, consistent information, and seamlessly integrate applications into business processes. [Outcome: 1] NOTE1: This practice is implemented by performing practices (control objectives) of the COBIT 4.1 Define the Information Architecture process with a specific focus on how governance supports internal control over financial reporting and business operation: **PO2.1 Create and maintain enterprise information model.** Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure. **PO2.2 Create and maintain enterprise data dictionary (ies).** Maintain an enterprise data dictionary that incorporates the organisation’s data syntax rules. This dictionary should enable the sharing of data elements amongst applications and systems, promote a common understanding of data amongst IT and business users, and prevent incompatible data elements from being created. **PO2.3 Establish and maintain data classification scheme.** Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption. **PO2.4 Manage data integrity.** Define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.

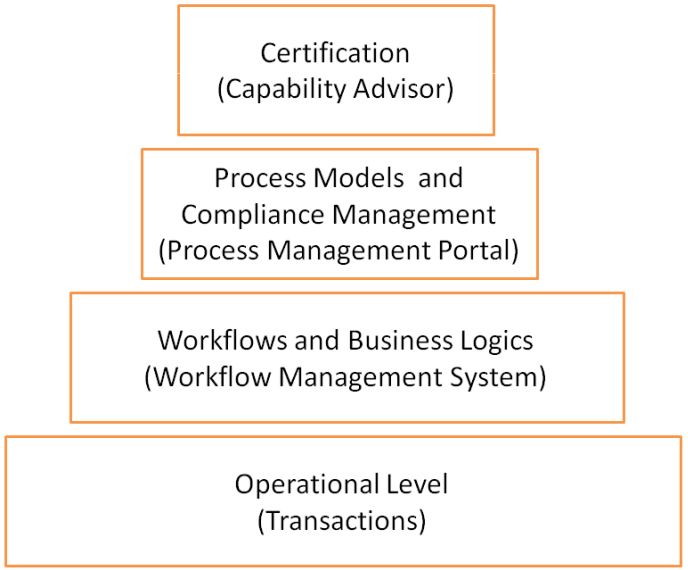
Information Reliability - Governance Process using COSO&COBIT

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

BPM GOSPEL: using multi-layer business assurance technology

Concept of 4 layers in BPM GOSPEL:

- Transaction Processing (e.g. payroll system-Memolux)
- ADAMAS Workflow/Control Management Tool (Gemma)
- Compliance/Audit Management – Stages ”Trusted Business” Edition (Method Park)
- Certification – Capability Adviser (ISCN)

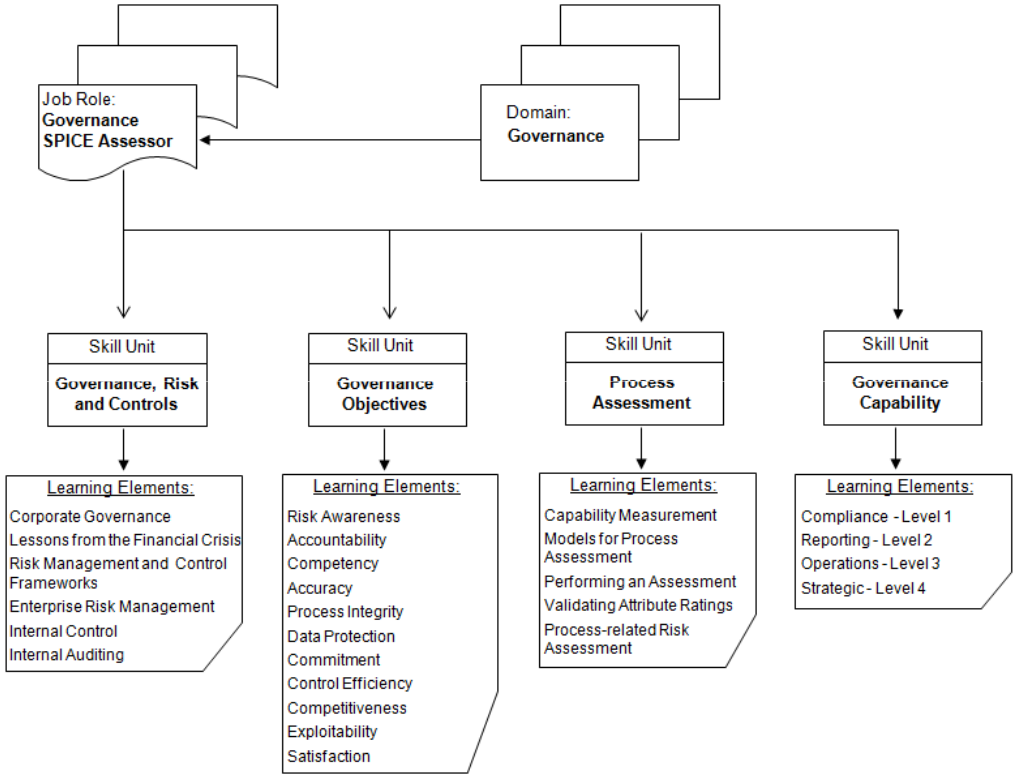


Implementing the Trusted Business Model by the BPM GOSPEL project - 1

- Case Studies for compliance management scenarios
  - Introduction to the relevant learning element based on the “Governance Objectives” skills definition
  - Summary of the business environment’s expectations concerning to the baseline business operation in context of the selected governance objective
  - Scope setting of the management assertions in context of the governance objective
  - Setting ”usefulness” and”effectiveness” metrics for enterprise goals
  - Use-case modelling by the Stages Special Edition for Trusted Businesses
  - Model based evidence collection by using Stages Compliance Workbench
  - Evaluation of compliance and governance capability profile by using Capability Adviser assessment reports

Implementing the Trusted Business Model by the BPM GOSPEL project - 2

- Approval of the extended Governance SPICE Assessor Skill Card by ECQA
  - JRC action plan
  - Skill Card implementatior
  - Training materials



- Formal procedure for evidence based examination by using coaching results

ECQA Job-roles related to Governance SPICE

- Internal Financial Control Assessor (from 2007)
  - Skill Card based on the COSO PRM
  - 800+ exams (Europe-wide)
  - Pool of ca. 600 multiple choice questions
- Governance SPICE Assessor
  - Skill Card developed (3 units covering GRC, Process Assessment and Governance Capability)
  - Training materials for IFCA trainers integrated with IFCA Moodle courses (training.ia-manager.org)
- ”Governance Objectives” Skill Unit (extended skill-card based on the Trusted Business Model)
  - Integrated training materials with Trusted Business case studies on the www.training.ia-manager.org
  - Evidence based testing is planned from 2012

ECQA for Trusted Business

- Current status
  - Qualification of Governance SPICE related job-roles, exam and training bodies
  - Certification for GSA & IFCA trainers and trainees
  - Promotion by ECQA portal and events
- For future
  - Evidence based testing using coaching results
  - Certificates for assessed companies (proposal for bylaw modification)
  - ECQA certified Trusted Business Advisors may feed a pool of qualified business units on a ”Trusted Business” portal, promoting their local activities and providing Europe-wide visibility
  - Reports in the Quarterly Journal published by ECQA

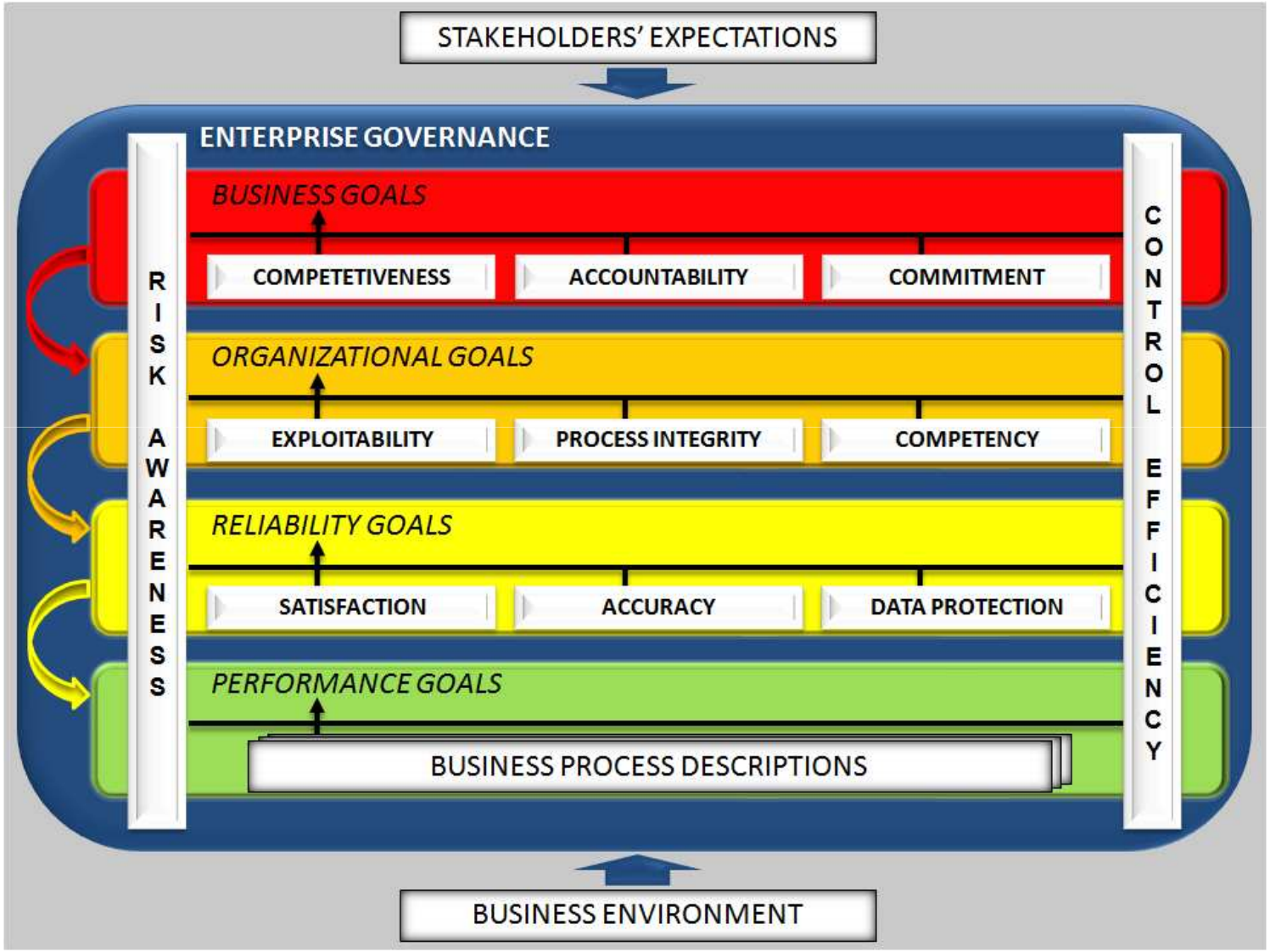
Proposal for a 2-level Qualification Scheme for Trusted Business Units

- Company (business unit) qualification for ”Trusted Business” trustmark
  - Acquiring personal skills related to the Trusted Business Model by coaching (model, tools, customization)
  - Evidence based examination for ECQA certification
  - Documented and validated self-assessment process referring to external evidences (e.g. provided by ”Stages Trusted Business Edition” platform)
  - Listed on Trusted Business Portal, trustmark usage
- Audit Report (external ISO/IEC 15504 assessment)
  - Using Capability Adviser platform (e.g. automatic evidence collection from Stages platform)
  - Assessment team (ISO/IEC 15504 Competent Assessor and Governance SPICE Assessor)
  - Publication (e.g. by a European Trusted Business Newsletter)

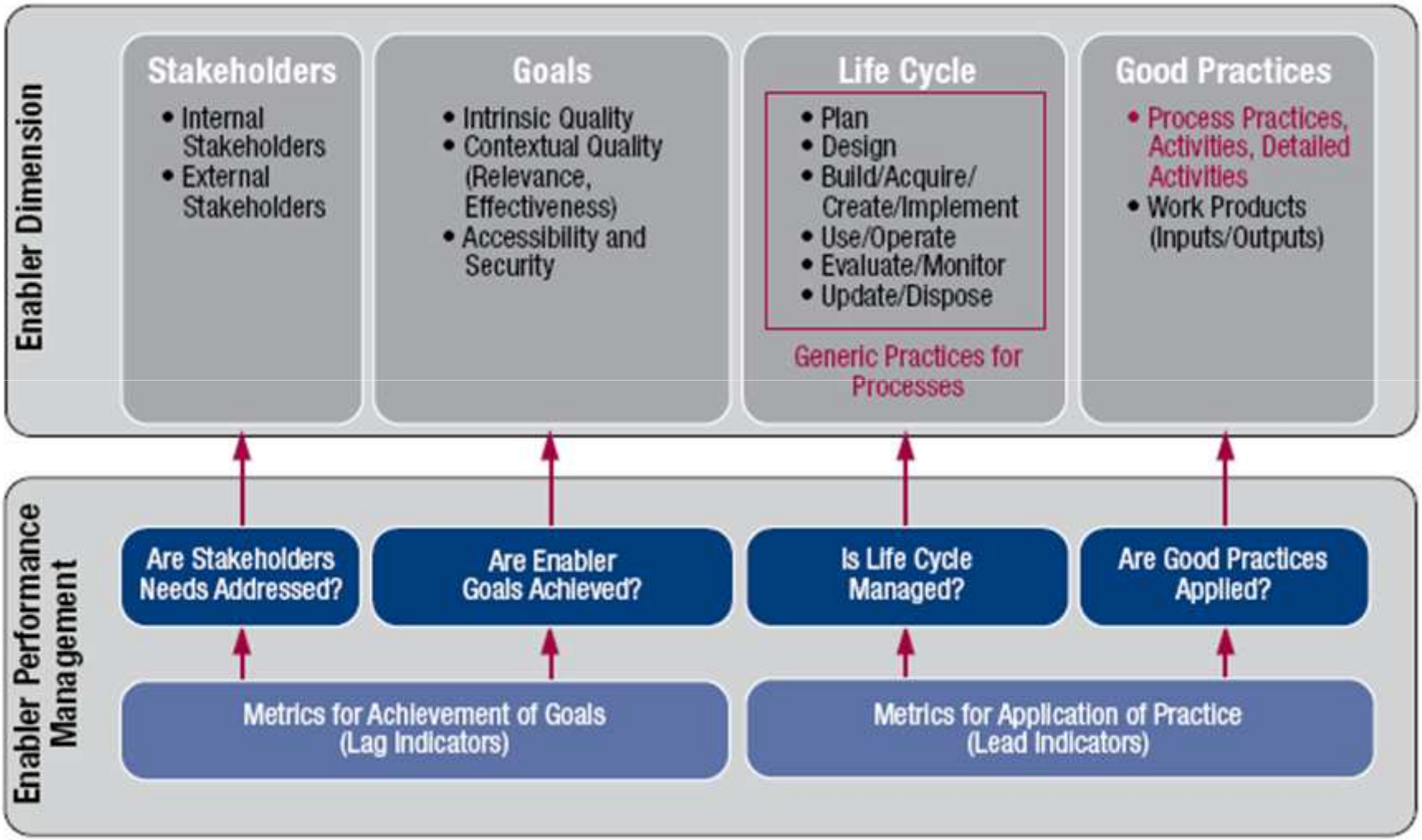
From Compliance Management to Operational Risk Management

- No evidence that compliance drives business success (on the contrary: all big failure companies having had long list of compliance and excellence records)
- Managing compliance issues has only limited focus on lower level outcomes (e.g. activity goals)
- Enterprise Governance should focus on internal and external contexts of risks (effects of uncertainties on enterprise objectives)
- Measurement is needed for establishing useful risk criteria for supporting management decisions at all organizational and operational levels
- Measurement also helps managing compliance scenarios for validating risk treatment options

Linking Governance Objectives to Enterprise Goals & Measures

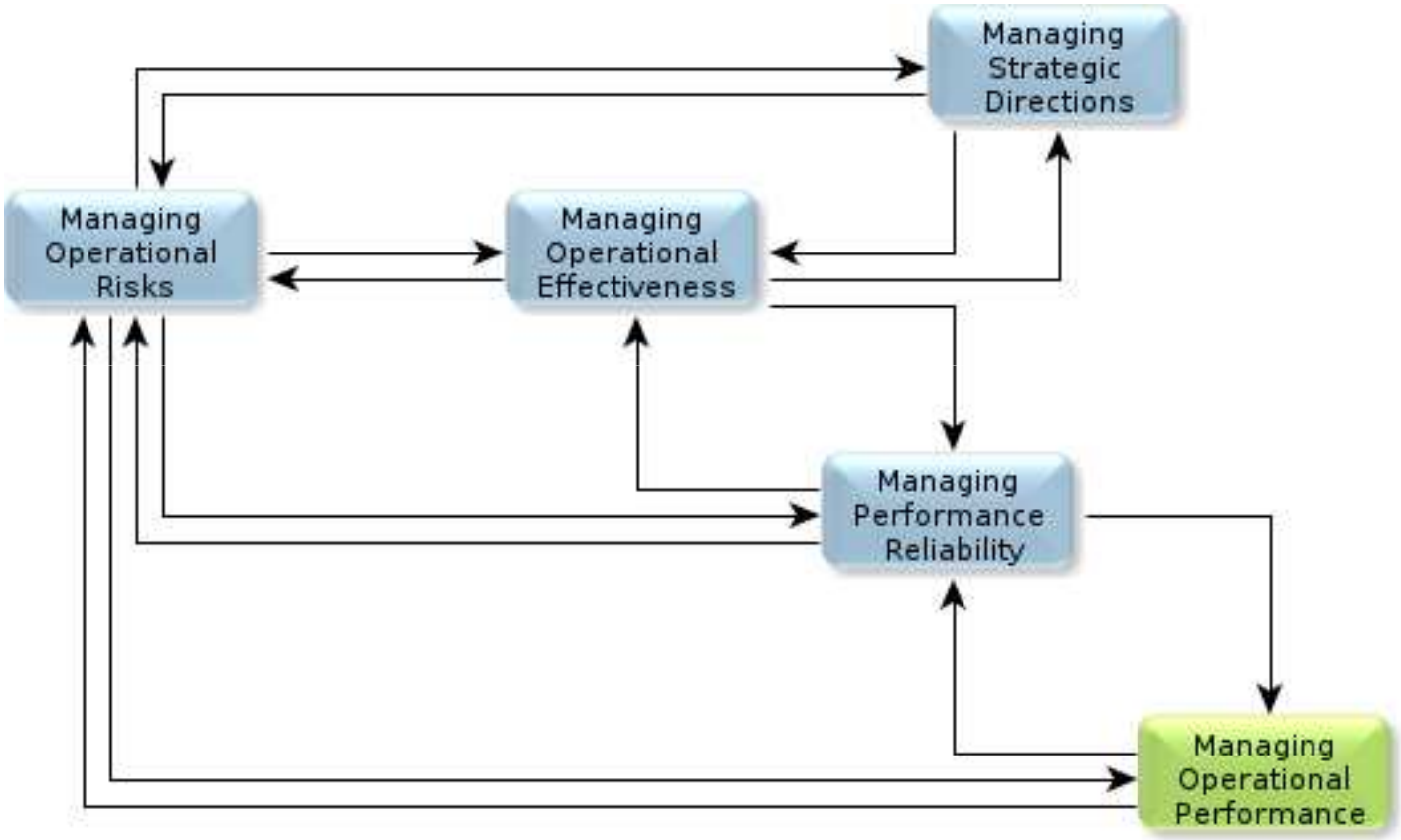


New Approach in COBIT5: Measurement of Enabling Processes



Source: COBIT® 5, figure 29. © 2012 ISACA® All rights reserved.

Governance Level 1: Performed Business Operation



Managing Operational Performance 1.

Managing Operational Performance of those business processes that are relevant to perform the business operation in compliance with internal and/or external expectations, rules or regulations.

Roles:

- Responsible: Operational Manager
- Support: Risk & Compliance Manager, Staff
- Inform: Business Line Manager

Scope: Level 1- Performed Business Operation

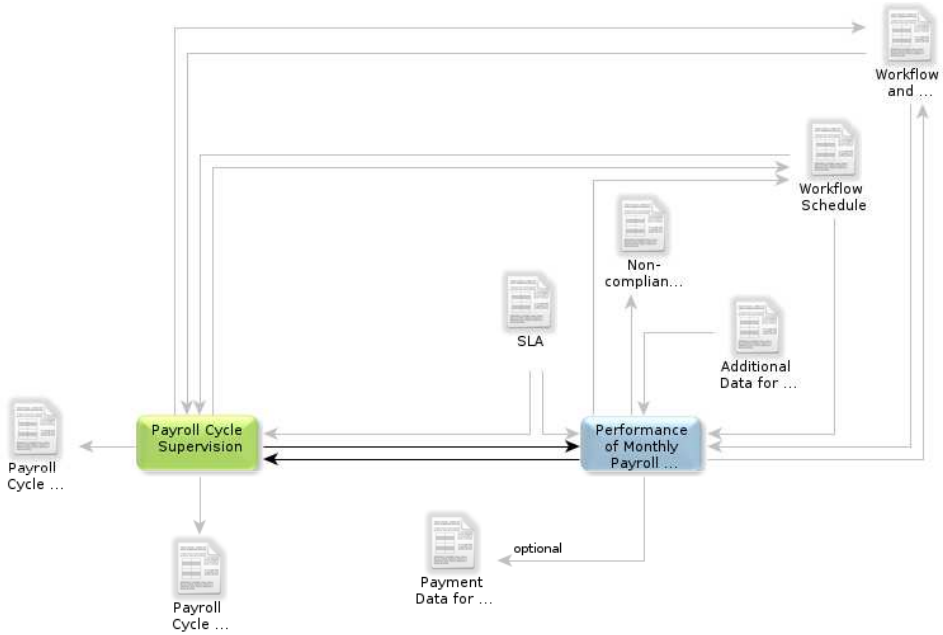
The organization demonstrates ability to manage performance of business processes that are relevant to support the organization's business operation.

Managing Operational Performance 2.

Outcomes: The process capability dimensions of the performed business processes enable 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.

Managing Operational Performance 3. Sample: Payroll Cycle Supervision



Roles
Responsible: Payroll Operation Manager
Support: IT contact, Payroll Controller, Payroll Clerk
Inform: Business Line Manager

Inputs
•Workflow Schedule
•Workflow and Document Tracking

Inputs from other Processes
•SLA

Outputs
•Workflow Schedule
•Workflow and Document Tracking

Outputs for other Processes
•Payroll Cycle Performance Report
•Payroll Cycle Control Summary Report

Description
Operational Management uses work-flow and documentation management system to supervise Monthly Payroll Calculation process activities and controls. Link to evidence

Managing Operational Performance 4. Sample metrics

Performance (”usefulness”)

Indicator: Performance Rate: *actual errorless calculations/planned calculations*

Time-horizon: operating cycles: *month of payroll processing*

Scale:

- approved major over performance: *over +10%*
- approved minor over performance: *+1-10%*
- approved performance at agreed levels: *+/- 1%*
- minor disapproval or indemnity: *1-5%*
- major disapproval or indemnity: *over 5%*

Expenditure (”effectiveness”)

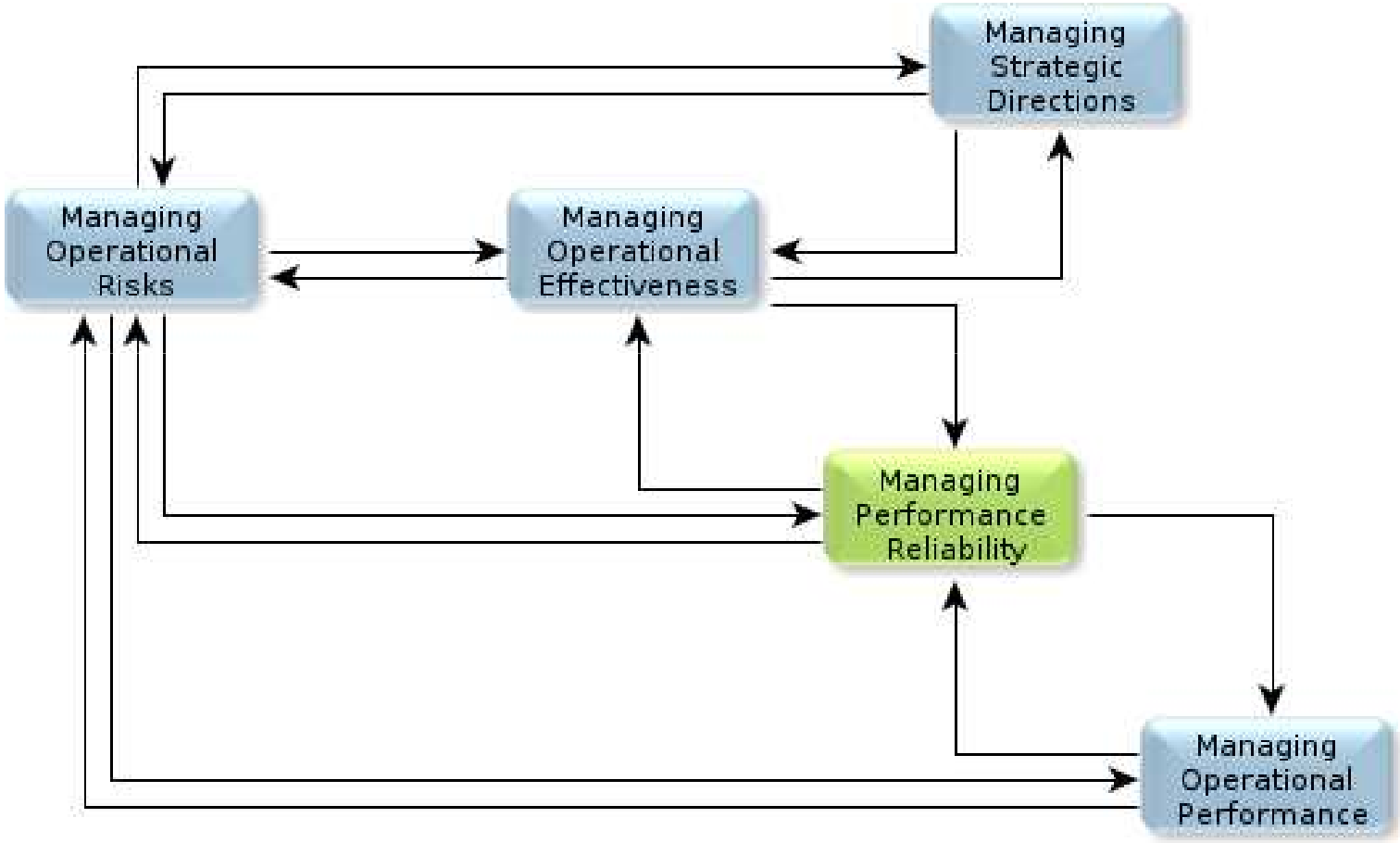
Indicator: Operating Costs: *hourly rate of payroll*

Time-horizon: operating cycles: *month of payroll processing*

Scale:

- significantly less than planned: *>15%*
- slightly less than planned: *5-15%*
- as planned: *+/- 5%*
- slightly more than planned: *+ 5-15%*
- significantly more than planned: over *+15%*

Governance Level 2: Reliable Business Operation



Managing Performance Reliability 1.

Managing Performance Reliability to achieve satisfaction and trust of users/customers regarding operational performance.

Roles:

- Responsible: Business Line Manager
- Support: Risk & Compliance Manager, Operational Manager
- Inform: Business Unit Leader

Scope: Level 2 - Reliable Business Operation

The organization demonstrates ability to fulfill performance reliability requirements of business operation.

Managing Performance Reliability 2.

Outcomes: By the support of related governance practices, 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.

Enablers:

- Adapting Satisfactory Operation practices
- Adapting Information Reliability practices
- Adapting Data Protection practices

Measures:

- Customer Retention (”usefulness”)
- Capacity Utilization (”effectiveness”)

Managing Performance Reliability 3. Sample metrics

Customer Retention (”usefulness”)

Indicator: Order Renewals

Time-horizon: contracting periods

Scale:

- extended orders
- intention to broaden (trust)
- affirmation (satisfaction)
- warnings (dissatisfaction)
- abandonment

Capacity Utilization (”effectiveness”)

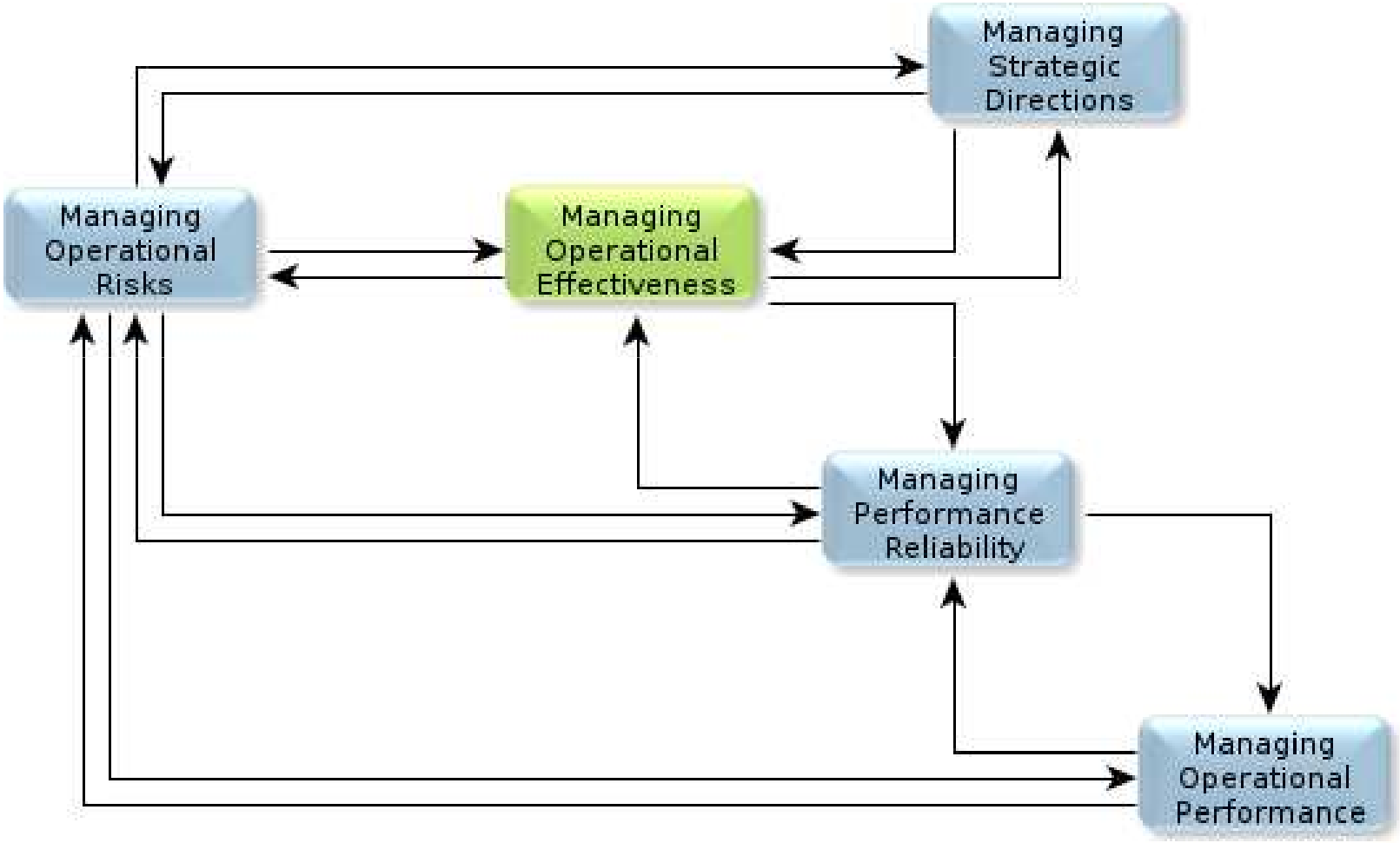
Indicator: Capacity Utilization Rate

Time-horizon: contracting periods

Scale:

- significantly better than planned
- better than planned
- as planned
- worse than planned
- significantly worse than planned

Governance Level 3: Effective Business Operation



Managing Operational Effectiveness 1.

Managing Operational Effectiveness to achieve specific operational performance objectives in alignment with organization's business goals.

Roles:

- Responsible: Business Unit Leader
- Support: Risk & Compliance Manager, Business Line Manager
- Inform: Executive Director

Scope: Level 3 - Effective Business Operation

The organization demonstrates ability to establish and achieve quantitative and qualitative performance objectives of business operation that are fundamental to support the organization’s relevant business goals.

Managing Operational Effectiveness 2.

Outcomes: By the support of related governance practices, 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.

Enablers:

- Adapting Exploitable Operation practices
- Adapting Process Control practices
- Adapting Competence Control practices

Measures:

- Profitability (”usefulness”)
- Agile Resource Allocation (”effectiveness”)

Managing Operational Effectiveness 3. Sample metrics

Profitability (”usefulness”)

Indicator: Operating Margin

Time-horizon: reporting periods

Scale:

- significantly over achieved
- moderately over achieved
- achieved as planned
- moderately underachieved
- significantly underachieved

Agile Resource Allocation (”effectiveness”)

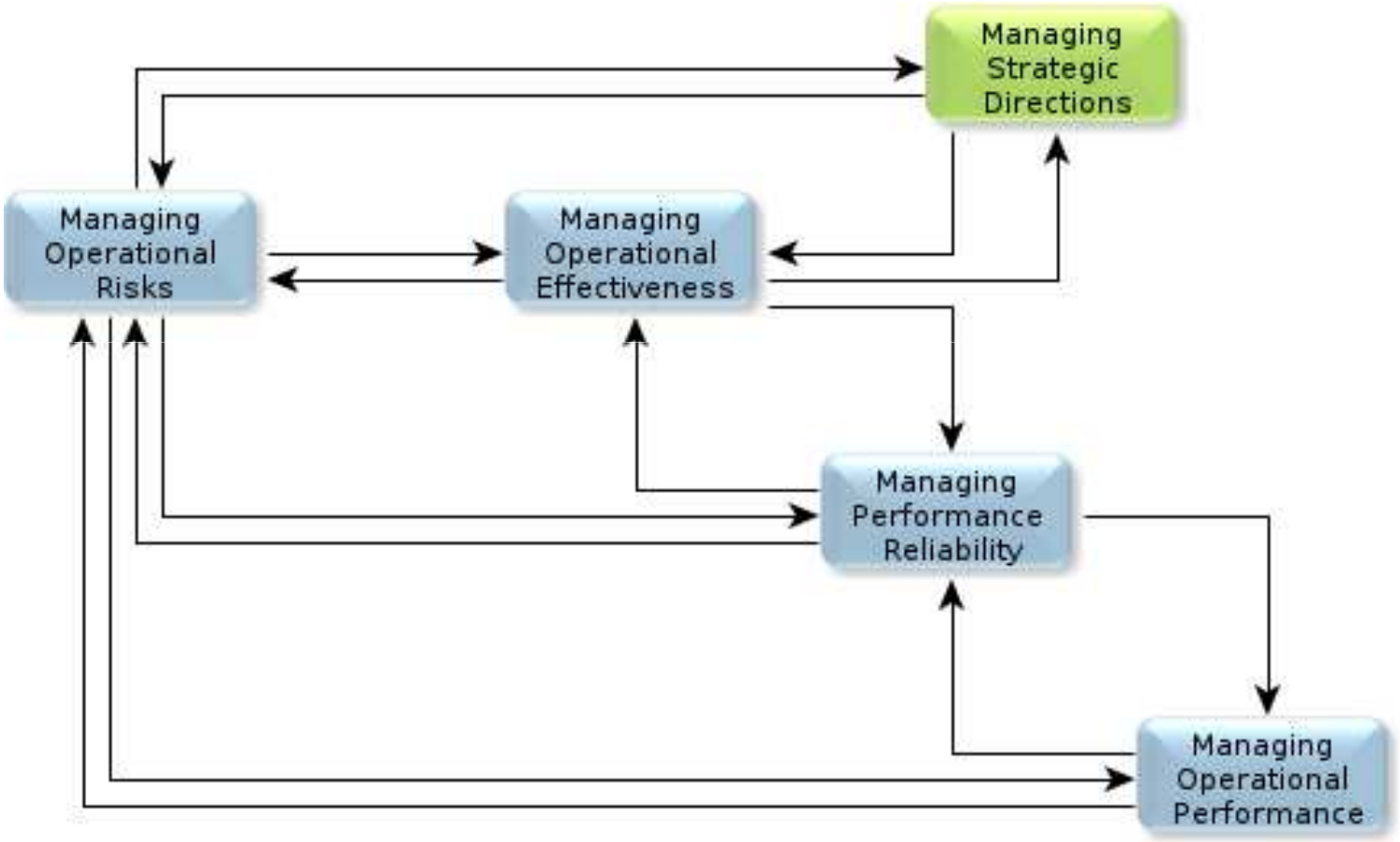
Indicator: Unit Cost

Time-horizon: reporting periods

Scale:

- very low variance
- variance within acceptable limits
- affordable variance
- more than affordable variance
- too high variance

Governance Level 4: Strategic Business Operation



Managing Strategic Directions 1.

Managing Strategic Directions in order to establish and maintain corporate commitment aligned with stakeholder's needs and expectations.

Roles:

- Responsible: Executive Director
- Support: Risk & Compliance Manager, Business Unit Leader
- Inform: Board, External Stakeholders

Scope: Level 4 - Strategic Business Operation

The organization demonstrates the ability to establish commitment for consistent and predictable performance of successful business operation aligned with strategic corporate objectives.

Managing Strategic Directions 2.

Outcomes: By the support of related governance practices, the organization:

- ensures market recognition of the business operation;
- makes management accountable for business operation in a way which is aligned with strategic corporate objectives;
- is committed to comply with ethical and integrity, business continuity and transparency requirements relevant to the stakeholders' needs and expectations.

Enablers:

- Adapting Competitive Operation practices
- Adapting Control Management practices
- Adapting Integrity Assurance practices

Measures:

- Business Goals (”usefulness”)
- Funding Resources (”effectiveness”)

Managing Strategic Directions 3. Sample metrics

Business Goals (”usefulness”)

Indicator: Revenues

Time-horizon: strategic planning periods

Scale:

- significantly over achieved
- moderately over achieved
- Achieved
- moderately underachieved
- significantly underachieved

Funding Resources (”effectiveness”)

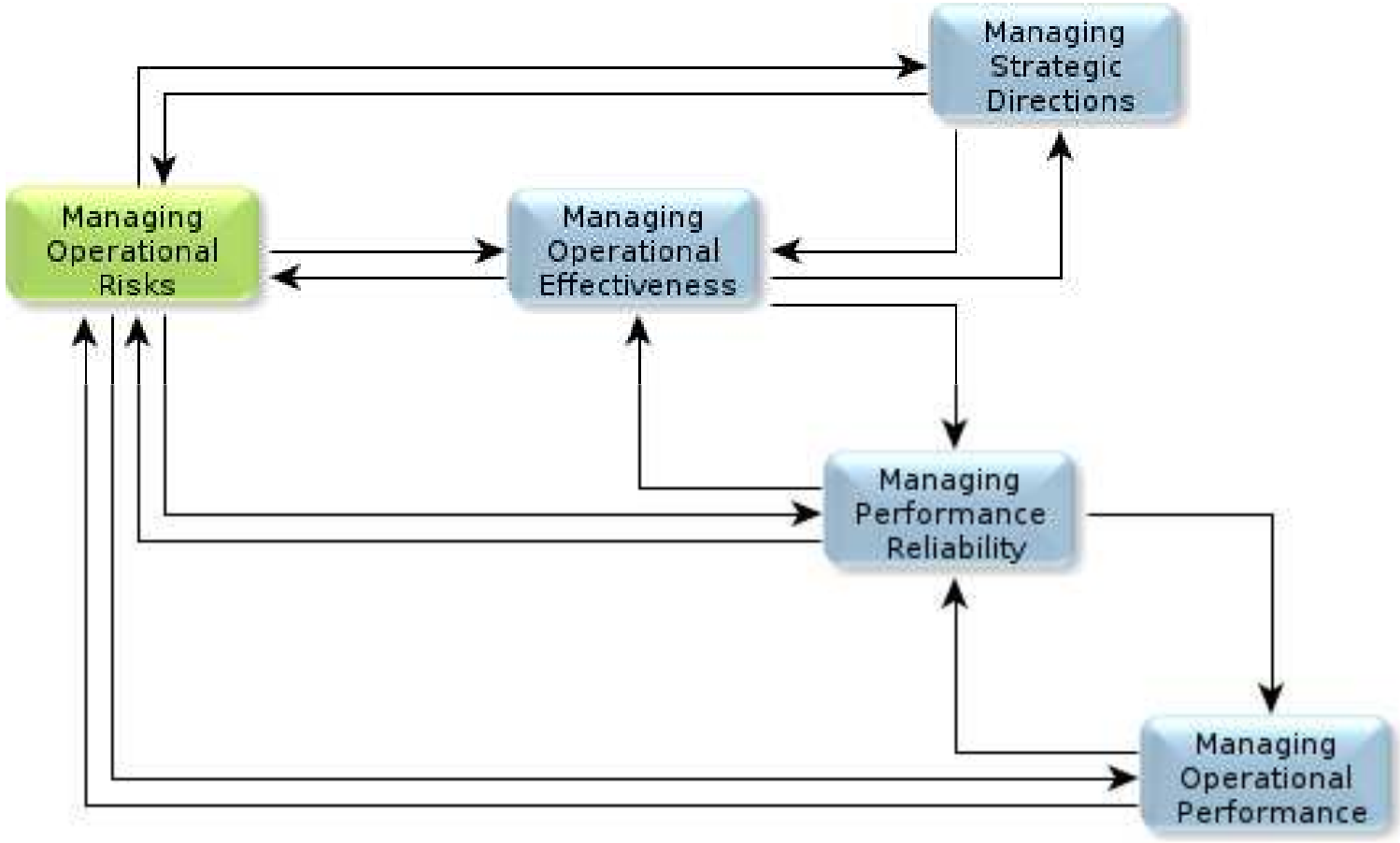
Indicator: Cash Flow

Time-horizon: strategic planning periods

Scale:

- available financial resources for approved requests over plan
- limited financial resources for non-planned requests
- financial resources are available for planned requests in a predictable manner
- availability of financial resources is less predictable or lagged behind the plan
- permanent and/or significant lack of financial resources

Enterprise Governance over Business Operation: Managing Operational Risks



Managing Operational Risks 1.

Managing Operational Risks to facilitate business operation in achievement of business goals.

Roles:

- Responsible: Risk & Compliance Manager
- Support: Trusted Business Advisor
- Inform: Board, Executive Director

Scope: Level 1-4 of Enterprise Governance

The organization demonstrates the ability to manage risks related to business operation that are fundamental to select and implement governance practices as risk treatment options leveraging achievement of organization's business goals established for business operation.

Managing Operational Risks 2.

Outcomes: By the support of related governance practices, the organization:

- takes communication and consultation with external and internal stakeholders during all stages of the risk management;
- establishes the internal and external context of business operation and risk management;
- identifies, analyzes and evaluates risks related to business operation;
- performs risk treatment cycles of providing or modifying controls and assessing their effectiveness against tolerable risk levels;
- takes periodic or ad hoc monitoring and review activities.

Enablers:

- Adapting Control Risks practices
- Adapting Control Efficiency practices

Measures:

- Effective Governance (”usefulness”)
- Consulting and Assurance Expenditure (”effectiveness”)

Managing Operational Risks 3. Sample metrics

Effective Governance (”usefulness”)

Indicator: Governance Capability Levels (actual vs. target)

Time-horizon: reporting periods

Scale:

- significantly over achieved
- moderately over achieved
- achieved as targeted
- moderately underachieved
- significantly underachieved

Consulting and Assurance Expenditure (”effectiveness”)

Indicator: Consulting and Assurance Costs

Time-horizon: reporting periods

Scale:

- significantly less than planned
- slightly less than planned
- as planned
- slightly more than planned
- significantly more than planned

Information and Contact

- www.governancecapability.com
- www.training.ia-manager.org
- www.ecqa.org
- www.trusted.hu (Hungarian)

Contact: János Ivanyos, ivanyos@trusted.hu

Thank you for your attention!