

# **Governance, Risk Management and Compliance (GRC): Business Process Transparency as a central component of a future-oriented GRC Solution**

Oliver Bauer

PROMATIS software GmbH  
Hamburg, Germany

## **Key Words**

Governance, Risk Management and Compliance (GRC), Horus Method, Business Modeling, Business Process Analyses, SOX, Basel II

## **Summary**

Increasingly strict legal guidelines and requirements on companies regarding their risk management and the transparency of their processes often call for the management to reconsider monitoring the compliance with corporate goals and their fulfillment.

The need to comply with directives and to recognize hazards related to risks and rule violations in time, to act promptly and effectively, may require more than individual IT-based solutions. The objective is to reduce and control so-called "information islands".

This paper gives a brief introduction to the concept of GRC and shows how a GRC solution can be implemented by using the Horus Method. The individual phases are presented and their contents are explained briefly. This method allows a fast and economical development of a comprehensive GRC solution.

# Content

<b>1</b>	<b>Introduction .....</b>	<b>3</b>
<b>2</b>	<b>The Horus Method: Conception of a GRC Solution based on Integrated Business Modeling .....</b>	<b>4</b>
<b>3</b>	<b>The Horus Phases and Models .....</b>	<b>5</b>
3.1	Phase 1: Strategy and Architecture Phase .....	5
3.2	Phase 2: Business Process Analysis .....	5
3.3	Phase 3: Target Concept and Process Implementation.....	6

# 1 Introduction

The world's rapidly increasing economic, environmental and computer-based crime requires increasingly complex regulations and monitoring. For a global company it is often not sufficient to consider only the national regulations for the company, but it has to consider all regulations that are affected in the context of transnational business. In parallel, investors and financial institutions demand effective risk management systems, e.g. through the establishment of early warning systems to detect risks and to create greater transparency within financial processes. Keywords here are SOX<sup>1</sup> and Basel II<sup>2</sup>. And the shorter half-life strategic decisions can only be met with safe and efficiently run business processes. In short, Governance, Risk and Compliance (GRC) issues are at the top of any management agenda.

The following article shows, based on experiences from already completed GRC projects, how Governance, Risk Management & Compliance solutions can be implemented based on methods and at low costs. The individual described themes outline one of the most important applications for business process engineering. The benefit of comprehensive business process models is enormous, precisely with GRC, because the majority of the requirements relate to the process quality and the transparency of business operations.

But first, a brief explanation of terms:

- **Governance**

Running a business based on clear and understandably formulated business objectives and instructions. Important conditions are legal compliance and completeness. Governance thus extends across all business sectors and levels, which is why we speak of horizontal and vertical governance.

- **Risk Management**

The sum of all measures for dealing with known and unknown internal and external risks. This includes the establishment of early warning systems to identify risks as well as measures to eliminate potential risks and to deal with occurred risks.

- **Compliance**

Refers to the fulfillment, correspondence or conformity with state laws and with rules and specifications, with principles (ethical and moral) and procedures as well as with standards (e.g. ISO) and conventions that are clearly defined. The compliance can be fulfilled either by means of coercion (e.g. by law) and/or voluntarily (e.g. adherence to standards).

---

<sup>1</sup> Der Sarbanes-Oxley Act (SOX) ist ein US-Bundesgesetz, das die Richtigkeit und Verlässlichkeit der veröffentlichten Finanzdaten von Unternehmen sicherstellen soll.

<sup>2</sup> Basel II describes the entirety of the regulations on capital that was drawn together by the Basel Committee on Banking Supervision. Since 2007 these regulations are binding in line with granting credits and credit trading for all financial services providers in the European States.

## 2 The Horus Method: Conception of a GRC Solution based on Integrated Business Modeling

The complete development and subsequent implementation of a comprehensive GRC approach is highly complex. This complexity is manageable only if easy-to-understand business models are used and when there is a systematic procedure for creating these models. The Horus Method is a suitable option. The models enable efficient forms of communication in the context of GRC project work. Horus provides a consistent documentation and supplies analysis and simulation approaches for quality assurance and optimization of analyzed business processes.

As for the diversity of the business requirements, Horus has the advantage that the generated models can be formally linked with each other (see Figure 1). Such an integrated business model prevents that with GRC new "information islands" are created, which can lead to inefficiencies and therefore stand in the way of interesting optimization possibilities.

It turns out that companies do not understand GRC primarily as a chore, but above all as an opportunity to optimize business processes, to achieve real cost savings with GRC and improve their competitive position.

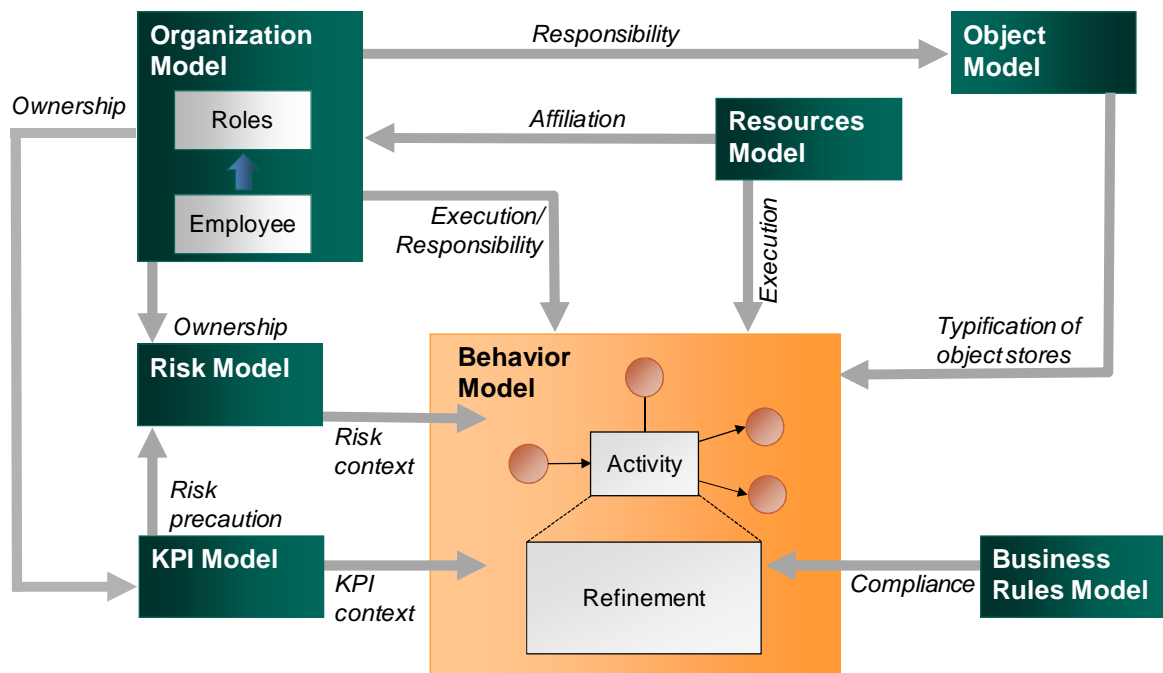


Figure. 1: Integrated business model without "information islands"

### **3 The Horus Phases and Models**

The involvement of all parties within the different phases of the GRC project is reached by using easy-to-understand graphic models. For this, in the respective phases, the powerful business process tool Horus Business Modeler offers the ability to create sub-models that are formally linked to a complete business model.

The advantage of the phase-oriented Horus Method is on hand: Depending on whether information has been obtained and documented in advance within the company, these can be considered. Under these circumstances, each phase in the process can be reduced and redundant work and costs are avoided.

#### **3.1 Phase 1: Strategy and Architecture Phase**

Within the strategy and architecture phase, aspects of strategic business management are worked out based on the Horus Method using a set procedure in the first step, to get an overview of the direction of the company, the current market position and existing risks. Here, the Horus Business Modeler supports specifically the important entry into a GRC project, where especially the management is involved.

Specifically, the following content and models within the strategic corporate management are worked out and presented graphically and are related to each other:

- Presentation of company objectives, based on visions and strategies (target model)
- Identifying the strengths and weaknesses, opportunities and threats for the company as part of a SWOT analysis (SWOT model)
- Derive critical success factors and strategies to achieve goals (strategy-/key indicator model)
- Collection of existing internal regulations and instructions (rule model)
- Comparison of regulations that are up to date and relevant to the company (e.g. in terms of risks, data protection laws, data access, HGB, etc.)
- First identification of risks (risk model)

#### **3.2 Phase 2: Business Process Analysis**

The information collected in collaboration with the management, which was documented by Horus, clearly shows after the first phase, where the potential for a company, but also where the weaknesses and risks lie.

Promoting strengths, to understand and correct weaknesses and risks. This GRC target can be quickly and easily implemented in the course of the Horus Method.

The already identified as possible critical areas from phase 1 will therefore be analyzed more in detail. Now, business processes, organizational structures, information systems and

object structures are represented graphically, analyzed in detail and, where appropriate, the models are simulated. Thus, vulnerability and therefore risks are identified and breaches of rules are detected.

Horus offers the possibility to visualize the processes and the associated detailed models in graphs in order to coordinate these with the affected areas. The aim is to investigate all business sectors in terms of deficits in the GRC management and carry out an initial verification of scheduled processes and systems against statutory provisions and rules. Gaps in compliance management, risk and antiquated governance structures are identified and "information islands" are documented.

By using the Horus Knowledge Bases it is possible to build up on pre-configured and quality-assured reference models and to adapt these according to the existing processes. This of course saves time and money in relation to the use and commitment of resources during the second phase.

The following content and models are worked out within the as-is analysis during phase 2, graphed and related to each other:

- Detailed analysis and presentation of existing business processes in the company with the aim to identify deficiencies or violations with regard to the compliance requirements (process model).
- The risks identified during the strategy phase are considered in detail and are completed, as these have a decisive impact on the achievement of goals and therefore on commercial success (risk model).
- The organizational structure of the company, which the individual processes are based on, is examined and illustrated (organization model).
- During the as-is analysis, concrete object graphs are generated and refined, as authorization concepts play an important role in the wake of GRC. Based on the object models, this can be analyzed and reported (object model).
- Existing internal rules and instructions will be analyzed in detail, visualized and examined. The model created in the preliminary phase is refined with the information obtained (rule model).
- The critical success factors and strategies are put in relation to corporate objectives and analyzed business processes and are detailed.

At the end of phase 2 the information gathered is reviewed with regard to compliance with the objectives to uncover violations of rules and laws or deviations from standards. These results are inter alia the basis for the subsequent target concept.

### **3.3 Phase 3: Target Concept and Process Implementation**

What are the major weaknesses, what are the serious violations of guidelines, rules or laws? Horus Method and the Horus components made clear no later than at the end of the

previous phase 2, what has been secretly feared in the company or in division lines. Now the acquired information has to be conceptualized and implemented into a GRC solution.

All processes recorded during the as-is analysis, which were identified as non-compliant to GRC, will now be considered with regard to optimization. In the processes, according to their complexity, the possible degree of rule violation is investigated, prioritized and processed. Not all processes must always be completely reorganized. For each individual case it is worked out whether the process has to be reorganized, or whether, for example, it is sufficient to draw up a report which provides information on compliance with a rule. But this has to be documented as a result at the end of the target conception, so that the individual model-based components can be transferred to the Horus GRC Manager, where they are used as the central cockpit for a future GRC management.

Therefore, phase 3 includes the following duties and activities with the aim to optimize the processes identified in the as-is analysis, which contain weaknesses and gaps in terms of GRC management, and to resolve "information islands":

- Acquiring and modeling optimized process development based on the Horus Knowledge Bases and findings from the verification, which guarantee that the procedures conform with laws and rules considering the given information systems (procedure model)
- Prioritization of process areas according to complexity and breach of the rules
- Design of future communication regarding compliance management
- Conceptual design of future risk strategies and regulations as well as monitoring mechanisms (risk model, rule model)
- Simulation of the target models (Horus simulation component)
- Transferring the Horus models into the Horus GRC Manager
- Identification and conceptual design of further GRC components to monitor identified risks and rules.

**Conclusion:**

With its modeling components and integrated procedure models, Horus offers the possibility to shape up companies in terms of Governance, Risk Management and Compliance. Accompanying synergy effects such as future cost savings and improving their competitive position are just two of many benefits that can be obtained here.

**Note**

The listed products are trademarked and belong to the respective owners.

Documentation release: June 2010

**PROMATIS software GmbH**

Pforzheimer Str. 160

76275 Ettlingen

Germany

Tel. +49 7243 2179-0

Fax +49 7243 2179-99

[info@promatis.de](mailto:info@promatis.de)

[www.promatis.de](http://www.promatis.de)