

# **Governance Risikomanagement und Compliance (GRC): Geschäftsprozess-Transparenz als zentraler Baustein einer zukunftsorientierten GRC-Lösung**

Oliver Bauer

Horus software GmbH  
Ettlingen

## **Schlüsselworte**

Governance, Risikomanagement und Compliance (GRC), Horus Methode, Unternehmensmodellierung, Geschäftsprozessanalyse, SOX, Basel II

## **Zusammenfassung**

Immer umfangreichere gesetzliche Vorgaben und Anforderungen an Unternehmen bezüglich Risikomanagement und Transparenz ihrer Prozesse erfordern oftmals ein Umdenken der Unternehmensführung in Bezug auf Überwachung der Unternehmensziele und Erfüllung dergleichen.

Die Notwendigkeit, Richtlinien einzuhalten und Gefahren in Bezug auf Risiken und Regelverstöße rechtzeitig zu erkennen, um zeitnah und zielgerichtet handeln zu können, erfordert mehr als nur einzelne IT-basierende Lösungen. Zielsetzung ist, sogenannte „Informationsinseln“ abzubauen und zu kontrollieren.

Der vorliegende Beitrag gibt eine kurze Einführung zum Begriff GRC und zeigt auf, wie mittels der Horus Methode eine GRC-Lösung implementiert werden kann. Hierbei werden die einzelnen Phasen mit ihren Inhalten kurz vorgestellt und erklärt. Diese Methode ermöglicht einen schnellen und kostengünstigen Aufbau einer umfassenden GRC-Lösung.

## **Inhaltsverzeichnis**

<b>1</b>	<b>Einführung .....</b>	<b>3</b>
<b>2</b>	<b>Die Horus Methode: Konzeption einer GRC-Lösung auf Basis einer integrierten Unternehmensmodellierung .....</b>	<b>4</b>
<b>3</b>	<b>Die Horus Phasen und -Modelle.....</b>	<b>5</b>
3.1	Phase 1: Strategie- und Architekturphase.....	5
3.2	Phase 2: Geschäftsprozessanalyse .....	5
3.3	Phase 3: Soll-Konzeption und Prozessimplementierung.....	7

## 1 Einführung

Die weltweit stark zunehmende Wirtschafts-, Umwelt- und Computerkriminalität verlangt nach immer komplexeren Regelwerken und deren Überwachung. Für ein global tätiges Unternehmen genügt es oftmals nicht, nur die nationalen Regelwerke am Firmensitz zu beachten, sondern es sind sämtliche Regelwerke zu berücksichtigen, die im Rahmen der länderübergreifenden Geschäftsprozesse tangiert sind. Parallel dazu fordern Investoren und Finanzinstitute ein effektives Risikomanagement-System, z.B. durch die Etablierung von Frühwarnsystemen zur Erkennung von Risiken und zur Schaffung einer größeren Transparenz innerhalb der Finanzprozesse. Stichworte hierbei sind SOX<sup>1</sup> und Basel II<sup>2</sup>. Und der immer kürzeren Halbwertszeit strategischer Entscheidungen lässt sich nur mit effizient geführten und sicheren Geschäftsprozessen begegnen. Kurzum: Governance-, Risiko- und Compliance-Themen (GRC) stehen in der Management-Agenda ganz oben.

Der nachfolgende Beitrag zeigt auf Basis von Erfahrungen bereits durchgeführter GRC-Projekte auf, wie Governance, Risikomanagement & Compliance-Lösungen methodengestützt und kostengünstig umgesetzt werden können. Die einzelnen beschriebenen Themen umreißen eines der wichtigsten Anwendungsfelder für Business Process Engineering. Der Nutzen umfassender Geschäftsprozessmodelle ist gerade bei GRC besonders groß, weil sich ein Großteil der Anforderungen auf die Qualität der Prozessführung und die Transparenz des Geschäftsbetriebs bezieht.

Zunächst aber eine kurze Begriffsklärung:

- **Governance**

ist die Führung eines Unternehmens auf Basis klar und verständlich formulierter Unternehmensziele und Handlungsanweisungen. Wichtige Bedingungen sind Gesetzeskonformität und Vollständigkeit. Governance erstreckt sich damit über alle Unternehmensbereiche und -ebenen, weshalb wir von horizontaler und vertikaler Governance sprechen.

- **Risikomanagement**

bezeichnet die Gesamtheit aller Maßnahmen zum Umgang mit bekannten und unbekanntem unternehmensinternen und -externen Risiken. Dazu gehört die Etablierung von Frühwarnsystemen zur Erkennung von Risiken ebenso wie Maßnahmen zur Beseitigung von Risikopotenzialen und zur Behandlung eingetretener Risiken.

- **Compliance**

bezeichnet die Erfüllung, Entsprechung bzw. Konformität mit staatlichen Gesetzen sowie mit Regeln und Spezifikationen, mit Grundsätzen (ethische und moralische) und Verfahren sowie mit Standards (z.B. ISO) und Konventionen, die klar definiert sind. Die Erfüllung der Compliance kann sowohl auf Zwang (z.B. durch Gesetze) als auch auf Freiwilligkeit (z.B. Einhaltung von Standards) beruhen.

---

<sup>1</sup> The Sarbanes-Oxley Act (SOX) is a US Federal law to protect investors by improving the accuracy and reliability of corporate disclosures.

<sup>2</sup> Basel II bezeichnet die Gesamtheit der Eigenkapitalvorschriften, die vom Basler Ausschuss für Bankenaufsicht zusammengetragen worden sind. In den EU-Staaten sind diese Vorschriften im Rahmen der Kreditvergabe und des Kredithandels seit 2007 für alle Finanzdienstleister verbindlich.

## 2 Die Horus Methode: Konzeption einer GRC-Lösung auf Basis einer integrierten Unternehmensmodellierung

Die komplette Erarbeitung und anschließende Umsetzung eines umfassenden GRC-Konzepts weist eine hohe Komplexität auf. Diese Komplexität ist nur beherrschbar, wenn einfach verständliche Unternehmensmodelle verwendet werden und eine systematische Vorgehensweise zur Erstellung dieser Modelle existiert. Die Horus Methode bietet sich hierfür an. Die Modelle ermöglichen effiziente Formen der Kommunikation im Rahmen der GRC-Projektarbeit. Horus sorgt für eine konsistente Dokumentation und liefert über Analysen und Simulationen Ansatzpunkte zur Qualitätssicherung und zur Optimierung der untersuchten Geschäftsprozesse.

Was die Vielfalt der fachlichen Anforderungen angeht, hat Horus den Vorteil, dass die erstellten Teilmodelle formal miteinander verknüpft werden können (siehe Abbildung 1). Ein derart integriertes Unternehmensmodell verhindert, dass mit GRC neue „Informationsinseln“ geschaffen werden, die zu Ineffizienzen führen und damit interessanten Optimierungsmöglichkeiten im Weg stehen.

Es zeigt sich, dass Unternehmen GRC nicht in erster Linie als lästige Pflicht, sondern vor allem als Chance zur Optimierung der Geschäftsprozesse begreifen, mit GRC echte Kosteneinsparungen erzielen und ihre Wettbewerbsposition verbessern können.

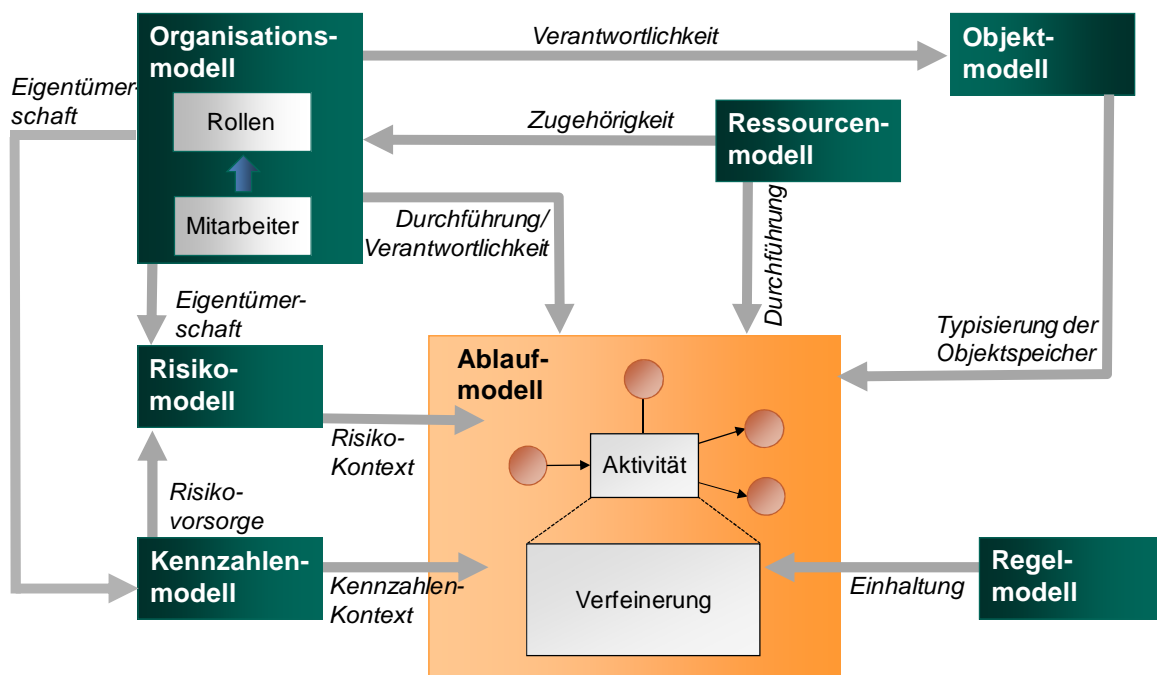


Abb. 1: Integriertes Unternehmensmodell ohne "Informationsinseln"

### 3 Die Horus Phasen und -Modelle

Die Einbindung aller Beteiligten innerhalb der unterschiedlichen Phasen eines GRC-Projektes wird durch die Verwendung einfach verständlicher grafischer Modelle erreicht. Hierzu bietet das leistungsfähige Geschäftsprozess-Tool Horus Business Modeler in den jeweiligen Phasen die Möglichkeit, Teilmodelle zu erstellen, die formal miteinander zu einem kompletten Unternehmensmodell verknüpft werden.

Der Vorteil der phasenorientierten Horus Methode liegt hierbei auf der Hand: Je nachdem, ob innerhalb eines Unternehmens bereits im Vorfeld Informationen gewonnen und dokumentiert wurden, können diese berücksichtigt werden. Dies kann u.U. die einzelnen Phasen im Vorgehen verkürzen sowie redundante Arbeiten und damit Kosten vermeiden.

#### 3.1 Phase 1: Strategie- und Architekturphase

Auf Basis der Horus Methode werden innerhalb der Strategie- und Architekturphase anhand eines festgelegten Vorgehens im ersten Schritt Aspekte des strategischen Unternehmensmanagements herausgearbeitet, um einen Überblick über die Ausrichtung des Unternehmens, die aktuelle Marktposition und bestehende Risiken zu erhalten. Der Horus Business Modeler unterstützt hier konkret den wichtigen Einstieg in ein GRC-Projekt, zu der gerade auch die Unternehmensführung einbezogen wird.

Konkret werden folgende Inhalte und Modelle innerhalb des strategischen Unternehmensmanagements herausgearbeitet, graphisch dargestellt und miteinander in Beziehung gesetzt:

- Darstellung von Unternehmenszielen auf Basis von Visionen und Strategien (Zielmodell)
- Feststellen der Stärken (strengths), Schwächen (weaknesses), Chancen (opportunities) und Bedrohungen (threats) für das Unternehmen im Rahmen einer SWOT-Analyse (SWOT-Modell)
- Ableiten von kritischen Erfolgsfaktoren und Strategien zur Zielerreichung (Strategie-/Kennzahlenmodell)
- Erfassung von bestehenden internen Regelungen und Anweisungen (Regelmodell)
- Gegenüberstellung von Regelungen, die für das Unternehmen aktuell und relevant sind (z.B. hinsichtlich Risiken, Datenschutzgesetzen, Datenzugriffen, HGB etc.)
- Erste Identifizierung von Risiken (Risikomodell).

#### 3.2 Phase 2: Geschäftsprozessanalyse

Die in Zusammenarbeit mit der Unternehmensführung gesammelten Informationen, die mittels Horus dokumentiert wurden, zeigen nach der ersten Phase deutlich, wo die Potentiale für ein Unternehmen, aber auch wo die Schwächen und Risiken liegen.

Stärken fördern, Schwächen und Risiken verstehen und korrigieren. Dieses GRC-Ziel lässt sich schnell und unkompliziert im Verlauf der Horus Methode umsetzen.

Die bereits als eventuell kritisch identifizierten Bereiche aus Phase 1 werden daher nun näher betrachtet. Dabei werden Geschäftsprozesse, Organisationsstruktur, Informationssysteme und Objektstrukturen graphisch dargestellt, detailliert analysiert und die Modelle gegebenenfalls simuliert. So werden Schwachstellen und damit Risiken identifiziert und Regelverstöße festgestellt.

Horus bietet hierzu die Möglichkeit, die Prozesse mit den dazu gehörenden Detailmodellen graphisch zu visualisieren, um diese auch mit den betroffenen Bereichen abstimmen zu können. Ziel ist es, alle Unternehmensbereiche im Bezug auf Defizite im GRC-Management untersucht zu haben und eine erste Verifizierung von erfassten Prozessen und Systemen gegenüber Gesetzesbestimmungen und Regeln durchzuführen. Lücken im Compliance-Management, Risiken und veraltete Governance-Strukturen werden identifiziert und „Informationsinseln“ dokumentiert.

Durch den Einsatz der Horus Knowledge Bases ist es möglich, auf vorgefertigte, qualitätsgesicherte Referenzmodelle aufzusetzen und diese gemäß den bestehenden Prozessen anzupassen. Dies erspart natürlich Zeit und damit Kosten im Hinblick auf den Einsatz und die Bindung von Ressourcen während der Phase 2.

Folgende Inhalte und Modelle werden innerhalb der Ist-Aufnahme in Phase 2 herausgearbeitet, grafisch dargestellt und miteinander in Beziehung gesetzt:

- Detaillierte Analyse und Darstellung bestehender Geschäftsprozesse im Unternehmen mit dem Ziel, Lücken oder Verstöße hinsichtlich der Compliance-Vorgaben zu identifizieren (Ablaufmodell).
- Die während der Strategieweise festgestellten Risiken werden näher betrachtet und vervollständigt, da diese entscheidenden Einfluss auf die Zielverfolgung und damit auch den Geschäftserfolg haben (Risikomodell).
- Die Organisations-Strukturen des Unternehmens, die den einzelnen Prozessen zugrunde liegen, werden untersucht und dargestellt (Organisationsmodell).
- Während der Ist-Aufnahme werden konkrete Objektdiagramme erstellt und verfeinert, da Berechtigungskonzepte im Zuge von GRC eine wichtige Rolle spielen. Auf Basis der Objektmodelle kann dies analysiert und erfasst werden (Objektmodell).
- Bestehende interne Regelungen und Anweisungen werden nun detaillierter analysiert, visualisiert und überprüft. Das in der Vorphase erstellte Modell wird mit den gewonnenen Informationen verfeinert (Regelmodell).
- Die kritischen Erfolgsfaktoren und Strategien werden in Beziehung zu Unternehmenszielen und analysierten Geschäftsprozessen gebracht und detailliert.

Zum Abschluss der Phase 2 findet eine Überprüfung der erfassten Informationen hinsichtlich der Compliance statt mit dem Ziel, Verstöße gegen Regeln und Gesetze oder Abweichungen von Normen aufzudecken. Diese Ergebnisse bilden u.a. die Basis für die darauf folgende Soll-Konzeption.

### 3.3 Phase 3: Soll-Konzeption und Prozessimplementierung

Was sind die großen Schwächen, was sind die schwerwiegenden Verstöße gegen Richtlinien, Vorschriften oder gar Gesetze? Spätestens zum Ende der vorausgegangenen Phase 2 wurde mittels Nutzung der Horus Methode und der Horus Komponenten transparent gemacht, was in Unternehmens- oder Abteilungsleitungen schon oftmals insgeheim befürchtet wurde. Nun gilt es, aus den gewonnen Informationen eine GRC-Lösung zu konzeptionieren und umzusetzen.

Alle Prozesse, die während der Ist-Aufnahme als nicht GRC-konform identifiziert wurden, werden nun hinsichtlich der Optimierung betrachtet. Dabei werden die Prozesse gemäß ihrer Komplexität und des möglichen Grades des Regelverstößes untersucht, priorisiert und bearbeitet. Nicht alle Prozesse müssen immer komplett umstrukturiert werden. Es ist im Einzelfall auszuarbeiten, ob dies zu geschehen hat, oder ob es beispielsweise auch ausreichend ist, einen Bericht zu erstellen, der Auskunft über die Einhaltung einer Regel gibt. Dies muss aber am Ende der Soll-Konzeption als Ergebnis dokumentiert sein, so dass die einzelnen modellbasierten Komponenten in den Horus GRC Manager überführt werden können, wo sie als zentrales Cockpit eines zukünftigen GRC-Management genutzt werden.

Die Phase 3 beinhaltet aus diesem Grund die folgenden Aufgaben und Aktivitäten mit dem Ziel, die während der Ist-Aufnahme identifizierten Prozesse, die hinsichtlich des GRC-Managements Schwachstellen und Lücken beinhalten, zu optimieren und Informationsinseln aufzulösen:

- Erarbeiten und Modellieren von optimierten Prozessabläufen auf Basis der Horus Knowledge Bases und Erkenntnisse aus der Verifizierung, die gesetzes- und regelkonforme Abläufe garantieren unter Berücksichtigung vorhandener Informationssysteme (Ablaufmodell)
- Priorisierung der Prozess-Bereiche gemäß Komplexität und Regelverstöße
- Konzeption zukünftiger Kommunikationswege hinsichtlich Compliance-Management
- Konzeption zukünftiger Risikostrategien und Regeln sowie zukünftiger Überwachungsmechanismen (Risikomodell, Regelmodell)
- Simulation der Soll-Modelle (Horus Simulationskomponente)
- Überführung der Horus Modelle in den Horus GRC Manager
- Identifizierung und Konzeption weiterer GRC-Komponenten zur Überwachung identifizierter Risiken und Regeln.

**Fazit:**

Horus bietet mit seinen Modellierungskomponenten und seiner integrierten Vorgehensmethode die Möglichkeit, Unternehmen im Hinblick auf Governance, Risikomanagement und Compliance fit zu machen. Begleitende Synergieeffekte wie zukünftige Kosteneinsparungen und eine Verbesserung ihrer Wettbewerbsposition sind nur zwei von vielen Vorteilen, die dabei erzielt werden können.

**Hinweise**

Die aufgeführten Produkte sind markenrechtlich geschützt und stehen dem jeweiligen Rechteinhaber zu. Stand der Dokumentation: Juni 2010

**Horus software GmbH**

Pforzheimer Str. 160  
76275 Ettlingen

Tel. +49 7243 2179-0  
Fax +49 7243 2179-99

info@horus.biz  
www.horus.biz