GRC²+ – The Formula for Sustainable Restructuring – Part 2: Minimum Standards for an Integrated GRC System

Introduction

This article sets out the minimum standards for an integrated GRC system (Governance, Risk, and Compliance) and offers practical guidance for implementation—particularly with a focus on small and medium-sized enterprises (SMEs).

As a conceptual foundation for the structures and processes needed to support sound corporate decision-making and execution, a (modified) GRC approach is recommended. This approach aims to address all key (and borderline) areas of business activity in a structured and integrated manner. The proposed approach also targets a commonly identified weakness in many existing efforts: the lack of measurable added value for the company relative to the resources invested. An integrated GRC framework can help overcome this issue.

From a cost-benefit perspective, senior management should also consider developing a GRC target pyramid. This begins with the definition of essential baseline standards. Over time, this foundation can be expanded to include industry-specific best practices and elements of "soft law", such as those found in Corporate Social Responsibility (CSR) frameworks.

Corporate Governance: The Framework for Effective Corporate Management

The framework of Good Corporate Governance comprises the full range of relevant laws, regulations, codes of conduct, mission statements, declarations of intent, and established practices in corporate leadership and oversight. It is largely shaped by legislators and owners.

Responsibility for designing the specific structure within this framework lies with the supervisory bodies and executive leadership. In addition to the company's constitution—such as the articles of association—there are strategic and operational documents that define the company's development and direction.

From this documentation, the company's organisational structure (management, supervisory bodies, departmental set-up, etc.) and core processes must be clearly derived. Ideally, these should be visualised through diagrams or organograms. Together with associated rules of procedure, these form the written foundation of governance within the business.

Like the risk and compliance management systems discussed below, governance follows a cyclical process—meaning both the organisational setup and documentation must be reviewed and, where necessary, updated on a regular basis.

Risk Management: Legal Obligations and Proven Standards

While there are no specific legal requirements governing the structure of a risk management system (RMS)—nor has case law provided detailed guidance—international and national standards often exceed what SMEs are expected to comply with. Nevertheless, these standards can be a useful benchmark during the design and implementation of an RMS.

A basic requirement for a legally compliant RMS is an integrated, rolling financial plan. This should include a monthly liquidity forecast extending over a minimum of 24 months, which also satisfies the legal framework of imminent insolvency as defined in §18 of the German Insolvency Code (InsO). In addition, the early warning guidelines published by the Federal Ministry of Justice under §101 of the StaRUG Act should be taken into account.

Such planning is typically embedded in the company's controlling processes, making Controlling a central pillar of the GRC system. Specific key performance indicators (KPIs)—such as the equity ratio or liquidity metrics—serve as early warning signals for potential risks.

The RMS also plays a crucial role in strategic development. Using tools like SWOT analysis, companies can evaluate risks ("Threats") and opportunities ("Opportunities") identified in the risk analysis, and derive appropriate control measures.

Compliance Management: Structural Minimum Standards

Similar to Governance and Risk Management, the structure of a Compliance Management System (CMS) is not prescribed by law. However, following the well-known "Neubürger decision" by the Regional Court of Munich, factors such as company size, industry, and business activity must be taken into account when designing a CMS.

While there are no concrete content-based requirements—such as those found in liquidity planning—structural minimum standards can be derived from established practice, including:

- IDW PS 980, which provides a framework for planning and implementing a CMS
- The DICO Working Paper A12, a modular compliance toolkit aimed at SMEs

In practice, it is clear that companies cannot avoid addressing core compliance topics such as tax law, employment law, and data protection. These areas must be assessed as part of a compliance risk analysis and appropriately incorporated into the CMS.

Integrating the Individual Systems into "GRC²+"

The GRC framework operates as a closed control loop, encompassing:

- Risk strategy
- Risk identification
- Risk assessment
- Risk control

This loop is reinforced by mutual oversight: the Compliance function ensures the RMS is legally compliant, while the Risk function evaluates the risks identified through the CMS.

In addition to content integration, organisational structure must also be considered. Companies can choose from various established models, such as:

- The House of Corporate Governance
- The Three Lines Model
- The COSO-ERM framework

For SMEs, a tailored structure is often more appropriate. In this model, Controlling serves as the foundation, with clearly defined interfaces to the Internal Control System (ICS) and Internal Audit (IA).

The ICS systematically implements rules to ensure compliance and prevent damage, while Internal Audit provides independent assessments of the effectiveness of both risk management and control processes. An overly close link between Risk Management and IA is generally discouraged—hence their clear separation in the Three Lines Model.

The "GRC²+" model presented here brings together Controlling, ICS and IA within a decision-focused GRC cycle to enable effective, integrated corporate management.