GRC²+ – The Formula for Sustainable Business Turnaround – Part 3: Guidelines for Implementing GRC in SMEs

Following the previous discussion on the minimum standards of an integrated GRC system (Governance, Risk & Compliance), this final section offers SME owners and managing directors some overarching considerations for effectively and efficiently building such a framework.

GRC as a Strategic Framework for Business

The "GRC triad" serves as a framework for documenting corporate culture and strategy. However, a GRC system can only be effective if the organisation's objectives are clearly defined. Strategy development and the implementation of compliance and risk management are interdependent processes.

A competitive business strategy must take legal and economic parameters into account, while risk and compliance strategies must, in turn, align with the company's strategic objectives.
To avoid drifting aimlessly through the GRC landscape, businesses should develop a GRC framework derived from their strategic planning. Existing components should be integrated iteratively. While certain requirements are dictated by law, other goals should reflect industry standards, cultural factors, and recognised best practices.

Corporate culture plays a pivotal role in shaping the GRC architecture: depending on whether an organisation leans towards a "high-trust" or "low-trust" culture, its GRC framework may vary significantly. CSR and ESG objectives can also be incorporated, forming a "GRC goal pyramid" that extends from basic legal requirements up to voluntary best practices.

The Role of Existing Structures and Processes

Very few companies are starting from scratch. Many already have established processes and structures that can be integrated into a GRC framework. Data protection, liquidity planning, and health and safety are often already in place and should be embedded within the broader GRC strategy. These existing "GRC islands" should be identified during the analysis phase and brought together in a systematic manner.

Strategic business planning forms the basis of any risk analysis. A fully integrated risk assessment serves as the foundation of the entire GRC² system.

From a Pragmatic Launch to a Stable GRC System

The implementation of a GRC system should begin pragmatically, aiming for early, tangible results. During the first cycle, the system completes its first run through the GRC process loop, achieving a basic level of compliance that satisfies legal minimum standards. With each subsequent cycle, identified weaknesses are addressed, leading to gradual stabilisation and optimisation. Over time, this results in a “settled” GRC system that operates efficiently and adapts continuously to evolving conditions.

A key success factor in this process is corporate culture. Trust takes time to build but can be lost quickly. Every GRC implementation must therefore take account of the company’s internal trust culture. This is especially important in SMEs, where personal relationships and a strong sense of identification with the business often play a more significant role than in large corporations.

Governance, Controls, and Sanctions as Success Factors

The quality of any GRC system ultimately depends on the people implementing it. Corporate governance is therefore a critical factor. A well-balanced allocation of GRC roles and oversight functions—such as advisory boards, supervisory boards, or external compliance officers—helps maintain equilibrium in company leadership. Strong oversight bodies are particularly vital in times of crisis, as they contribute to overall stability.

Trust is essential—but so is oversight. Even in trust-based SME environments, effective control mechanisms are necessary to ensure regulatory compliance. The internal control system (ICS) is a core component. The extent to which this goes beyond the "four-eyes principle" will depend on the organisation's specific structure. However, early integration of the ICS and internal audit into the governance framework is highly recommended.

To embed new rules into the corporate culture, breaches must be met with appropriate consequences. A tiered sanctions framework for compliance violations ensures proportional responses. In addition to legal liability rules for directors, companies should also establish incentives for the adoption and maintenance of GRC structures, as positive reinforcement often proves more effective than punishment. At the same time, a clear distinction should be drawn between consequences and sanctions to avoid excessive penalisation and preserve the organisation’s trust culture.

Efficiency, Acceptance, and Continuous Improvement

Successful digitalisation relies on the prior standardisation of processes. The “art of omission” should serve as a guiding principle to eliminate inefficiencies. Clear rules must also be established for monitoring digital systems and processes.

A GRC system is only as strong as its weakest link. A lack of awareness among employees can compromise its effectiveness. Regular communication and training are therefore essential for conveying measures and objectives transparently. These training initiatives should be firmly embedded within the GRC process cycle.

Once the GRC system has stabilised, the focus should shift to simplification. Policies and procedures should be reviewed periodically and streamlined where necessary to prevent unnecessary complexity.

Long-term acceptance of a GRC system depends on its demonstrable value to the business. Companies should define GRC-relevant key performance indicators (KPIs), ideally linked to core financial metrics such as profitability. Quantifying the value of a compliance management system can improve both acceptance and effectiveness.

Final Thoughts

This study highlights that, despite common management errors in the German SME sector, the development of adequate governance systems has progressed too slowly. The GRC²+ model provides an integrated framework that connects governance, risk, and compliance management, counteracting the formation of organisational silos. An effective GRC system must support informed decision-making, deliver measurable benefits, and continuously adapt to evolving business processes.

Especially in turnaround or restructuring scenarios, evidence of a functioning, integrated GRC framework is increasingly seen as a prerequisite for absolving management of liability. Businesses that have already implemented such systems are in a stronger position to maintain competitiveness and better protect themselves against enterprise risks. However, implementation requires not only structural adjustments but also a cultural shift and the ongoing education of all stakeholders to ensure lasting efficiency and effectiveness in corporate decision-making.
Without the implementation of an integrated governance framework, it will likely become increasingly difficult for directors, restructuring experts, and insolvency practitioners to rely on the business judgement rule in future.