

GRC and CSR/ESG as a management tool

Josef Scherer

Since GRC frequently has negative connotations as “joy and impact free pooling of monitoring and control functions” (“lines of defence”) in practice, it has been suggested that we ought to consider replacing GRC with new terms such as “DRM” (digital risk management) and “IRM” (integrated risk management) [see Lie-Bjelland 2020].

Rather than constantly inventing new terminology that is not widely recognised, it would make more sense to promote the new meaning of GRC, which is now gradually becoming established in business organisations across the world, as more of an evolution / advancement of the concept. The meanings of controlling, internal control system (ICS), risk and compliance management have experienced similar changes in recent years.

Global trends: Governance, sustainability and cyber risk management

The DIN standard committee 175-00-01 AA is currently developing ISO 37000: 2021 Guidance for the Governance of Organizations. There are also numerous current standards in the sphere of sustainability, corporate social responsibility (CSR) and environmental social governance (ESG), for example the Global Reporting Initiative, at UN and OECD level and at national level [see Scherer/Kollmann/Birker 2019]. Now that major companies have an obligation to provide sustainability reports and it is compulsory for the report to assess their business partners for sustainability, the combined sustainability and annual report is also starting to become more established among SMEs.

Linked to exponential development in digitalisation, the issues of cyber risk management and information security are currently mandatory objectives of corporate governance that complies with all obligations.

Ineffective but expensive GRC systems, IT tools and methods

In practice, the (IT) tools, systems and methods used frequently result in nothing more than additional bureaucracy, time and financial expense and do not actually deliver any value contribution (example: “Risk accounting” with Excel, PowerPoint and Word).

In many cases, (IT) solutions recommended by consultants are uncritically implemented. Although they are suitable to satisfy checklists of minimum requirements for audits, attestations and certificates, they do nothing to improve culture, awareness, expertise or processes (“a fool with a tool is still a fool...”) [see Lie-Bjelland 2020].

Lack of measurable value contribution

Ultimately most managers, and also consultants, are unable to give a convincing and motivating explanation of the verifiable and measurable value contributions provided by GRC / ESG. A major insurance company recently pointed out huge increases in liability risks for companies, not just due to a large number of product recalls.

Because of the cognitive distortions experienced by managers rooted in behavioural economics, this “subconscious awareness”

leads to unease, fear of assuming responsibility and “signs of paralysis in the face of pending decisions”, but not to implementation of a legally compliant organisation that releases the business from liability and “freeing up management and employees for entrepreneurial behaviour”.

The level of maturity in process management that can be found in various organisations and companies, but also in individual departments, differs massively. However, good process management is the basis for digitalisation, information security and sustainability as part of an integrated GRC management system.

GRC and CSR/ESG as a management tool at senior management level

GRC is not the exclusive privilege of corporate departments or public officials. In actual fact, GRC with CSR/ESG has to gain a foothold as a standard element of day-to-day strategic and operational activity by management, senior managers and employees alike.

Step 1: Sound analyses including “materiality analysis”

The manager (executive director, CEO, supervisory board member) has to use a range of (risk) analyses and a “materiality analysis” (based on GRI) to assess the current megatrends, the economic and financial position, resilience and sustainability of their organisation and, most importantly, has to come up with appropriate objectives and strategies.

Objectives can be achieved using a digitalised and integrated GRC management system.

Step 2: Definition of top level of objectives, strategies and drivers of resilience and sustainability using “materiality analysis” and “management approach”

The question arises on which top level issues a business leader has to or should concentrate [see Scherer 2020]. The “materiality analysis” focuses on economic, environmental and societal issues that are of interest both to the organisation and to its stakeholders. To ensure competitiveness and sustainability, a particular management approach is adopted. This sets out the responsibilities and rules, targets, performance indicators and measures (projects and initiatives) for achieving the overall objectives. The key issues cover the minimum requirements set out in section 267a of the German Commercial Code (HGB). To supplement this, the sustainability report is produced based on the Global Reporting Initiative (GRI) standard [see Scherer 2021].

Example top level objectives developed using a materiality analysis

- Ensuring sustainable long-term survival and increasing the company's value.
- Customer and stakeholder satisfaction.
- Compliance and legally compliant organisation,
- (Project-related) Risk management,
- Strategic human resource development,
- Resource conversation,
- Digitalisation and information security.

Alongside the other departmental objectives, these are then broken down into process and employee objectives. Even for identification and decision making on top issues, GRC with risk and compliance management provides valuable information by highlighting legal requirements, limits, risks and opportunities. For each of the strategic objectives set out above, there is an appropriate "management system island" to ensure that the objectives are achieved. Ideally, these should be combined as an integrated (GRC) management system.

The importance of data, risk and compliance management methods for good business decisions is emphasised by the new international ISO standard ISO DIS 37 000: 2020 on "Governance of organisations" (7.8 Information and decisions).

Digital or semi-automated decision support with GRC and the rules of the business judgement rule (section 91 Para. 1 sentence 2 of the German Companies Act (AktG)) is currently gaining a foothold in all sectors [see Scherer, 2020].

Step 3: Regulation of responsibilities

As in process management, when it comes to the management approach used for the relevant top level objectives, the RACI method with definition of responsibility for performance (Responsible), responsibility for content (Accountable), incorporation of expert knowledge (Consulted) and reporting lines (Informed) is recommended.

Step 4: Identification of requirements in terms of the top level objective

Compliance management deals with identification, assessment and measures to satisfy various requirements from legislation, legal decisions, technical clauses, contracts, standards etc. in terms of the relevant top level objective.

Step 5: Developing and planning strategies

Objectives and the means adopted (strategies) to reach the objective are subject to uncertainty: Risk and opportunity management helps with modern methods, for example scenario analyses and bandwidth simulation, for heading in the right direction.

Step 6: Derivation of projects / measures with management and monitoring

Particularly with (project-based) risk management, the "lines of defence" ensure optimised achievement of objectives in the projects / initiatives adopted by managing the uncertainties (risks / opportunities).

Step 7: Stakeholder communication / sustainability reporting

The stakeholders are informed, including through the annual sustainability report. What is less well known among decision makers and the authors of annual reports is that untruths can be met with criminal sanctions. DRS 20 now demands that these reports contain relevant facts, not empty platitudes.

Summary and outlook

Sustainable and value(s)-based investments are in greater demand than ever on the financial market. Some investors now only finance companies that use appropriate indicators and satisfy comprehensive criteria in the social and environmental fields [see PWC 2020]. At the same time, digitalisation, sustainability and GRC are creating transparency and structure.

Digital optimisation of processes and methods also provides huge scope for less resource-intensive working [see Scherer 2021, p.13]. But one problem remains. How do we manage to get the new significance of GRC and CSR/ESG for value contribution and achievement of objectives into the heads of decision makers and other employees? At a cognitive level, we are faced with the challenge that managers and employees allow (behavioural economics) the new significance of GRC and CSR/ESG to be understood and applied. However, even if they understand the advantages of GRC intellectually, motivation (ideally intrinsic) still has to be created at an emotional level for them to want to fully practice GRC and CSR/ESG.

Literature

- Lie-Bjelland, O. [2020]: *Das fehlende P in GRC [The Missing P in GRC]*, <https://www.risknet.de/themen/risknews/das-fehlende-p-in-grc/>, downloaded on 14 January 2021.
- Scherer, J., Kollmann, P., Birker, A. K. [2019]: *Integriertes Nachhaltigkeits-Managementsystem [Integrated sustainability management systems]*, [scherer-grc.net](https://www.scherer-grc.net)
- Scherer, J. [2020]: *Resilienz und Zukunftsfähigkeit – GRC als „Klammer“ diverser Management-Inseln [Resilience and sustainability - GRC as a collection of various management islands]*, <https://www.risknet.de/themen/risknews/grc-als-klammer-diverser-managementsystem-inseln/>, downloaded on 14 January 2021.
- Scherer, J. / Fruth, K. / Grötsch, A. [2021] (eds.): *Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ [Digitalisation, sustainability and "corporate management 4.0"]* Deggendorf 2021.
- PWC [2020]: *The growth opportunity of the century, Luxembourg 2020.*



Autor

Prof. Dr. jur. Josef Scherer
Lawyer, Regional court judge,
Internatoinal Institute for Governance,
Management, Risk and Compliance Management,
Deggendorf Institute of Technology
and member of the FIRM advisory council