Prof. Dr. Josef Scherer

Lawyer, Board member of the International Institute for Governance, Management, Risk and Compliance Management of the Deggendorf University of Technology. Member of various ISO/DIN standards committees (governance, compliance, human resources management) and Austrian Standards International (risk management system).

„Management reloaded” -
„GRC & ESG in Strategy & Performance”
(GRC & ESG in S & P)

Linking digitization and information security, sustainability (ESG/CSR)[1] and "Corporate Governance 4.0" (GRC)[2] with strategy, target achievement and (sustainability-) reporting[3]

Summary

„The times, they are a-changin’” (Bob Dylan)

When, if not now?

Disruptive environmental developments such as Corona, new working environments, digital transformation with increasing information security risks, technology change, sustainability trends (ESG/CSR), legal and regulatory requirements, and many more require the conscientious decision-maker (executive board, managing director, supervisory board) to derive appropriate goals, strategies, and measures.

It is not only since COVID-19 that everyone has been talking about resilience and sustainability. In practice, however, the maturity of the process organization, the "Tone from the Top" and the competencies of management and employees are still lagging far behind.

The question arises which companies will survive the (Corona) crisis, which are resilient and sustainable – and therefore interesting for stakeholders.[4]

„The answer, my friend, is blowin’ in the wind” (Bob Dylan)

Prerequisites for the successful concept of how the topics of digitization, sustainability and "Corporate Governance 4.0" (GRC) can be linked with strategy, performance and business reporting:

"GRC" respectively „ESG (CSR)“ must finally be properly understood, desired and applied: Not as an "annoying monitoring function", but as a modern and indispensable corporate management tool.
The special thing about it: Done correctly, this saves time, money and stress, already during the implementation – and not only years later!

Note: The article contains links to external third-party websites over whose content we have no influence. Therefore, we cannot assume any liability for these external contents. The respective provider or operator of the pages is always responsible for the content of the linked pages. The linked pages were checked for possible legal violations at the time of linking. Illegal contents were not recognizable at the time of linking.
However, a permanent control of the contents of the linked pages is not reasonable without concrete evidence of a violation of the law. If we become aware of any infringements, we will remove such links immediately.

[1] ESG: Enviromental, Social, Governance. CSR: Corporate Social Responsibility.

[2] Governance, Risk and Compliance

[3] Cf. in detail on the topic of this paper: *Scherer* in *Scherer/Fruth/Grötsch* (eds.): Digitalisierung, Nachhaltigkeit und "Unternehmensführung 4.0", 2021. extract at scherer-grc.net/publikationen

[4] Cf. *Scherer*, Resilienz & Zukunftsfähigkeit, GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de

An important prerequisite for this knowledge is:
The “new GRC-approach” is almost the same like the “Environmental, Social, Governance-approach (ESG/CSR).”

„GRC & ESG in S & P!“[5]

1. Definitions

„He said Captain, I said what?” (Captain Sensible)

What does GRC respectively ESG/CSR and Integrated GRC / ESG- (CSR-) -Managementsystem mean?[6]

Governance, risk and compliance "together", i.e. **"GRC"** respectively ESG (CSR), may be something other than the sum of the three components. There is no legal definition here. GRC respectively ESG (CSR) could be translated (unfortunately somewhat complex) as "Integrated, sustainable, compliance-oriented and risk-based corporate governance and monitoring".[7]
A management system[8] that digitizes several corporate functions or processes (e.g., risk, quality, environmental, occupational safety and compliance management) and integrates them into a "corporate management system" can be called **"Digitalized Integrated GRC GRC / ESG- (CSR-) -Management System".**[9]

[5] Cf. *Scherer* in *Scherer/ Fruth / Grötsch* (Ed.): Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“, 2021, S. III.

[6] Cf. *Scherer/Fruth* (Ed.), Governance-Management Volume I, 2014, p. 9 and Volume II, 2015, p. 30, as well as Scherer, Good Governance und ganzheitliches strategisches und operatives Management.
Die Anreichung des „unternehmerischen Bauchgefühls“ mit Risiko-, Chancen- und Compliance Management, Corporate Compliance Zeitschrift (CCZ), 6/2012, p. 201, free download available on Scherer-grc.net/Publikationen.

Corporate governance means "Adequate interaction between the institutions [shareholders, management (board /executive director) and supervisory board (supervisory board / advisory board)] as well as proper corporate governance and supervision". Governance is more than management. Governance should also include corporate social responsibility (CSR) with economic, social and environmental sustainability) and integrity/ethics. See. ISO/DIS 37000:2020 Governance of organizations

Sustainability (ESG/CSR) could be described as " aligned decision-making and action with preserving progress ".

Risk management deals with uncertainties in decision-making and goal achievement.
It helps to identify, evaluate and manage threats (and opportunities).

Compliance means dutiful conduct with regard to generally binding rules (laws, case law), but also with regard to (internal) requirements declared to be binding [e.g., regulations from the "Code of Conduct" (company-specific rules of conduct) or employment contract].

[7] The reason why governance must be compliance-oriented: Compliance is generally the legal, compelling framework for corporate action.
Corporate management must be risk-based, because otherwise it would not act like a "conscientious" entrepreneur, board of directors, managing director: identifying, evaluating and controlling threats (and opportunities) is a prerequisite for achieving goals.

[8] Structural and procedural organization consisting of components (responsibilities, roles, tasks and areas of responsibility, for example mapped in organizational charts, job descriptions, etc. as well as process flows, delegations and interactions, etc.) with the purpose of supporting an organization in decision-making, goal setting and planning, implementation as well as control and monitoring to achieve mandatory and optional goals set.

[9] Cf. *Scherer / Fruth / Grötsch* (ed.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC), 2021, p. 23.

No old wine in new hoses

Since "GRC" respectively ESG (CSR) often has negative connotations in practice as a "fun- and impact-free bundling of monitoring and control functions" ("lines of defense"), GRC is to be replaced by new terms such as "DRM" (Digital Risk Management) and "IRM" (Integrated Risk Management).[10]

In my opinion, it would make more sense not to constantly "invent" new terms that are only known in isolated cases, but to propagate the new meaning of "GRC", which has gradually established itself worldwide in the corporate organization, in the sense of an evolution / further development.
In the same way, the meanings of "controlling", "internal control system", risk and compliance management have also changed in recent years.[11]

2. Global trends: Governance (GRC), Sustainability (ESG/CSR) and Cyber-Riskmanagement

DIN's standards committee 175-00-01 AA is currently developing **ISO 37000: 2021** ***Guidance for the Governance of Organizations.***[12]

According to this, the **core area of governance** will include the following points:

1. Mission, values, culture
2. Sustainable value creation
3. Strategy
4. Legal framework[13]
5. Responsibility[14]
6. Stakeholder-relationship
7. Leadership and values[15]
8. Data and decisions[16]
9. Risk-based corporate governance[17]
10. Social responsibility[18]
11. Sustainability[19]

[10] Cf. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de: *" IRM was introduced by Gartner in 2017 to address the increasingly complex needs associated with digitization, cybersecurity and risk management. Gartner is launching a modified concept that reaffirms the inherent positive aspects of GRC under a new name while eliminating the negative association." Gartner is a very prominent and influential "vendor that provides market research and analysis on IT developments."*

[11] For example, risk management lege artis is no longer accepted as mere risk accounting; rather, consistent quantification and aggregation is now mandatory (IDW PS 340 : 2020).
Similarly, compliance is no longer limited to anti-corruption and antitrust law, as it was in the early days (about 2005).
[12] The author is considered an "expert", as a member of the relevant working group of DIN/ISO WG 309.
[13] Compliance: Laws, standards, rules, guidelines.
[14] „Fit & proper" competences, transparency and trust.
[15] Values and lead the organization sustainably, ethically and effectively.
[16] Data as a valuable resource for decision preparation and felling.
[17] Control uncertainties regarding strategic objectives.
[18] Social responsibility (CSR / ESG).
[19] Economic social and environmental value creation.

Important: These “GRC-items” are the *same items* which ESG/CSR adress:

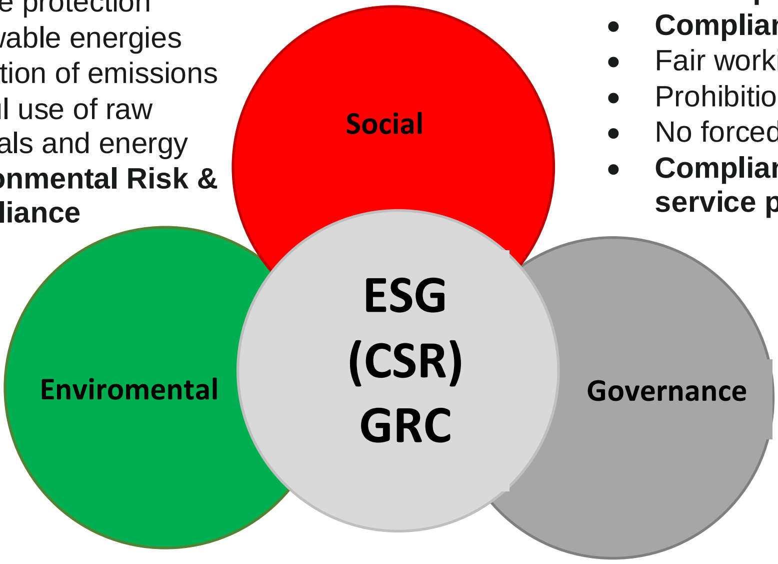
What is the famous „ESG”?

Environmental

- Environmental protection
- Climate protection
- Renewable energies
- Reduction of emissions
- Careful use of raw materials and energy
- **Environmental Risk & Compliance**

Social

- **Occupational safety**
- **Health protection**
- **Compliance with labor law**
- Fair working conditions
- Prohibition of child labor
- No forced labor
- **Compliance with ESG criteria for service providers and suppliers**



Governance

- Ethical **corporate governance**
- **Compliance**
- **Anti-Bribery**
- **Independent Supervisory Board**
- **Risk management**

Figure. 01: Enviromental-Social-Governance-ESG[20]

Sustainability reporting[21]

In the field of sustainability respectively **corporate social responsibility (CSR/ESG),** [22] there are also numerous very up-to-date standards (e.g., Global Reporting Initiative) on UN, OECD and national issues.[23]
Now that the "big" companies have become obligated to report on sustainability and the report also obligates them to check their business partners for sustainability, the combined sustainability and annual report is also gaining ground in the SME sector.[24]

[20] Cf. Euramco, last accessed on 14.01.2021, https://www.euramco-asset.de/glossar/environmental-social-governance-esg/

[21] Mandatory sustainability reporting - the so-called CSR reporting obligation, based on EU Directive 2014/95/EU - was introduced in Germany in 2017 for capital market-oriented companies with more than 500 employees, EUR 40 million in sales and/or total assets of EUR 20 million (Section 289 HGB).
This non-financial corporate reporting is based on the guidelines of the Global Reporting Initiative (GRI) and must be included in the management report, cf. *Scherer / Fruth / Grötsch* (Ed.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC), 2021.
The minimum requirements that must be addressed in the sustainability report are environmental, social and employee concerns, respect for human rights and the fight against corruption.
Numerous individual laws and case law deal with sub-areas of CSR and sustainability that must be observed, for example: environmental law, labor law, occupational health and safety law, criminal law and the law on administrative offenses, and much more.
Thus, a compliance and human resources management system already represents a significant and essential part of CSR and sustainability. If an environmental and energy efficiency management system is also integrated here, a large part of the requirements of the CSR / sustainability management system should be fulfilled.

[22] Environmental, social, governance

[23] Cf. *Scherer, Kollmann, Birker* Integriertes Nachhaltigkeits-Managementsystem, 2019, for free download on scherer-grc.net/Publications.

[24] BMW set a good example in 2019 (combined sustainability and annual report).

Cyber risk management and information security

Along with exponential digitization, the topics of "Cyber risk management" and "Information security" (ISO 27000 ff.) are currently also mandatory goals of dutiful corporate management.

3. Pain / Problems

Forrester[25] states *"unprecedented changes in business and technology require much more sophisticated, strategic and proactive GRC capabilities."* [26]

Notwithstanding this, in practice, "business as usual" can be observed in response to the lighting up of all the "lines of defense warning lights"[27] as with Penny in The Big Bang Theory:

Leonard's mother: *"Your check engine light is on"* Penny: *"Yeah, I gotta put a sticker over that."*[28]

"Nobody likes to play with grubby kids!" - Reasons for negative sentiment towards "GRC" respectively ESG (CSR):

Ineffective but complex GRC/ESG- (CSR-) systems, IT tools and methods

Often, (IT) tools, systems and methods are still used in practice, which only mean additional bureaucracy, time and financial effort and do not add any value (example: "risk accounting" with Excel, PowerPoint and Word...).[29]

Ticking off "regulatory checklists" instead of good business decisions ("Governance")

Another aspect: (IT) solutions recommended by "youth research consultants" are often implemented uncritically, although they are suitable for meeting the minimum requirements for audits, tests and certifications set out in checklists.

However, culture, awareness, competencies, processes are not improved ("a fool with a tool is still a fool...").[30]

Lack of measurable value contributions (Impact / Performance) of GRC respectively ESG (CSR)

Finally, most managers, but also consultants, are not able to explain in a convincing and motivating way what demonstrable, measurable value GRC respectively ESG (CSR) brings. The argument that GRC respectively ESG (CSR) - makes corporate activity possible in the first place,

- helps to avoid problem cases that might occur,
- fulfills regulatory requirements,
- reduces liability risks,
- promotes the achievement of corporate goals,
- etc.,

sounds trite and does not contain the proof that GRC respectively ESG (CSR) financially improves performance (P) within a reasonable period of time.[31]

[25] Also, like *Gartne*r, an opinionated company that "provides market research and analysis on IT" (Wikipedia).

[26] Cf. *Lie-Bjelland*, Das Fehlende P in GRC, 9 / 2020, Risknet.de.

[27] Reason or cognitive bias: "Nothing bad has happened yet...".

[28] Cf. https://www.youtube.com/watch?v=PWBfJr2kxhc

[29] Cf. *Lie-Bjelland*, Das felhende P in GRC, 9 / 2020, Risknet.de:
"Ineffective and worthless GRC systems
One observation is that although GRC is one of the most important disciplines for running a successful business, few, if any, poor methods and technologies exist to adequately support it. Indeed, Excel and even Word and Power Point were among the most commonly used software technologies to support the risk management, compliance management and governance needs of the enterprise. The capabilities required to enable a sustainable, efficient and effective GRC program that is aligned with strategy and performance are simply not present in such tools and will ultimately result in a lack of value and non-effectiveness. This results in GRC having a negative reputation among senior leadership."

[30] Cf. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de:
"Check-box compliance and a necessary evil.
(...) shortcomings of companies in terms of good corporate management ("corporate governance"). Many regulators have failed in this area (...). It is worth noting that traditional GRC is often associated with check-box compliance and is a necessary evil that leads a company to focus only on the absolute minimum compliance requirements - simply to pass a possible audit."

[31] Cf. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de.

Achleitner, a luminary in the field of "Private equity and investment", also believes that "Corporate governance is becoming / is an important value driver":

"If you look at the levers of value creation over the past 30 years, improving operational value creation has been the most important. (...) "Operational value creation will be the biggest challenge for companies (...) in the future. (...) In the past years, corporate governance was often under the monitoring aspect. The value-creating aspect, on the other hand, was missing. ***It is about better corporate decisions*** *through functioning and lived governance (...). Good corporate governance practice will be a decisive competitive factor in the future (...) from the investment practice they hear that there are* ***cases in which corporate governance contributes two thirds of the increase in value of the companies. (…)"***[32]

Unfortunately, here there is also no concrete example with details of euros, dollars or bit coins that proves what the increase in value is based on.

People and managers like to suppress regulatory requirements and liability risks ...

Due to some prominent cases (not just "Wirecard"), word is spreading very quickly that many things that were tolerated or not consistently pursued in the past are now being severely punished.[33]

The "perceived" increase in liability and sanctions for board members, managing directors, supervisory board members and even shareholders and employees accused of having acted in breach of duty can be measured objectively: In the 10-year period 1986-1995, there were as many managerial liability convictions as in the previous 100 years.
For the subsequent 10-year periods 1996-2005 and 2006-2015, a further doubling was measured or estimated![34]

Recently[35], a large insurer pointed to enormously increasing liability risks for companies, not only because of a large number of product recalls.

Currently, *supply chain legislation and corporate sanctions law* in the legislative pipeline are causing further anxiety among business leaders.

Due to the behavioral-economic cognitive biases in managers, this "awareness in the back of the head" leads to discomfort, fear of taking responsibility, and "paralysis before upcoming decisions," but not to the implementation of a detachable legally compliant organization that takes the load off management and employees for corporate behavior.

Although in recent times case law[36] and legislators (cf. e.g., Section 153 of the German Fiscal Code: "Tax Compliance") have confirmed the generally recognized legal concept that organizational precautions to avoid breaches of duty may, in individual cases, render the accusation of intentional action superfluous.
The draft law of the Federal Ministry of Justice[37] on corporate sanctions for compliance violations also follows this direction.[38]

"A third observation and my key point is the missing P in GRC. OCEG.org, the inventor of GRC, states that "successful achievement of principled performance requires coordinated capabilities that address performance against objectives, risks arising from uncertainty, and compliance with both mandatory and voluntary requirements - each with consideration for the other. (...) From an external perspective, there is no gap between business strategy, strategic execution, and operations, and the market doesn't care whether the CEO's explanation for the risk event was unpreparedness, ignorance, or more likely a statement demonstrating ignorance."

[32] Cf. *Achleitner* Corporate Governance als Werttreiber in Handelsblatt, 6/2015, p.28.

[33] My former professions as a public prosecutor and judge and my current professional activities as a lawyer in commercial (criminal) matters and, for almost 20 years, as an insolvency administrator, compliance ombudsman, external compliance officer or consultant in the area of governance, risk and compliance (GRC) have a common denominator: all functions take care prophylactically of dutiful behavior of entrepreneurs, managers and employees or reactively of compliance violations.

[34] Cf. *Scherer, Resilienz und Zukunftsfähigkeit - GRC als „Klammer" diverser Management-Inseln*, 9 / 2020, Risknet.de.

[35] Cf. dpa from 9.9.2020, Allianz: Liability risks for companies are increasing.

[36] Cf. The first decision of the Federal Court of Justice on the deferral effect and for the benefit of a (certified) compliance management system, see Federal Court of Justice of 09.05.2017 Az. 1 StR 265/16, *„KMW"* Rn. 110

[37] Draft bill: Act on the Promotion of Integrity in Business from June 2020

[38] Cf. *Scherer*, Resilienz und Zukunftsfähigkeit - GRC als „Klammer" diverser Management-Inseln, 9 / 2020, Risknet.de

Overburdening management and employees in digitization, information security and GRC respectively ESG (CSR) due to low maturity of process management

The level of maturity of process management found in the various organizations / companies, but also in individual departments, varies greatly. However, good process management is the basis for digitization, information security, sustainability in the Integrated GRC Management System:

"State of the art" (e.g., in IT security law, data protection or occupational health and safety) is no longer Excel, e-mail floods, data graveyards, but (partially) automated processes and human workflow management.

If only "non-lived analog documents" are digitized, in the end there are only "non-lived digitized documents", but no lived networking, automation and digital transformation in the sense of "4.0".
Integrated human workflow management systems are necessary for a "real digital transformation”.[39]#

4. Solutions for new goals and key performance indicators

"What you measure affects what you do. If you don't measure the right thing, you're not doing the right thing."[40]

GRC respectively ESG (CSR), properly used as a management tool at management level

GRC is not an exclusive privilege for staff units or officers. Rather, GRC must be incorporated as a matter of course into the daily strategic and operational activities of management / executives / employees.[41]

Step 1: Well-founded analyses incl. "Materiality analysis"

The manager (executive board, managing director, supervisory board) must assess the current megatrends
(risk) analyses and a "materiality analysis" (according to GRI) to assess the current megatrends, the economic and financial situation, the resilience and future viability of his organization and, above all, to derive appropriate goals and strategies.
Goals can be achieved with the help of a digitalized and integrated GRC management system, consisting predominantly of goals, processes, tools and methods, as well as the culture and competencies of managers and employees.
In many companies, this results in a partly changed business model or even an increased "intellectual performance" (intellectual property / digital assets), which consists of knowledge in the form of processes with associated components (roles, goals, resources), IT systems and IT tools, algorithms, robots and, in the remaining places, people with appropriate competencies and attitudes.[42]

Porter/ Nohria[43] point out that the *“CEO's job has become more difficult because the scope and breadth of tasks are increasing, organizational structures are becoming more complex, technical progress is progressing, competitive pressure swells, and CEOs' responsibilities are constantly growing."*

Therefore, they recommend:

[39] Cf. *Scherer*, Resilienz und Zukunftsfähigkeit - GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de.

[40] Cf. *Joseph Stiglitz*, Nobel Laureate in Economics, 2018, in connection with the development of alternative measurement methods for the state of a country. The reason for this was the criticism of measuring and comparing wealth above all through gross domestic product.

[41] Cf. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de: *From the back bench to the boardroom - More and more companies are taking advantage of (...) because they have experienced how integrated GRC can impact their performance. They are moving risk and compliance management in an enterprise context from the back bench to the boardroom to achieve a holistic view of their risk profile and bridge the gap between strategy, strategic execution and operational silos, and they are leveraging both regulatory and voluntary compliance from a selection of readily available, proven best practice frameworks to drive corporate performance and value."*

[42] Cf. *Scherer / Fruth / Grötsch* (Ed.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC), 2021.

[43] Cf. *Porter/ Nohria*, How *„CEOs“* manage time, download on internet, 2018

- The CEO has to ensure a clear and well-defined strategy in every organizational unit and in the company as a whole.

- The same applies to adapting the organizational structure of the company to the strategy as a prerequisite for appropriate decisions.
- Effective bosses establish well-designed processes that help everyone make good decisions. They serve as a basis for information, support, empowerment and an increase in the level of competence.[44]

Most corporate activities will be carried out in the future as predominantly or partly digitized processes.

Processes and a digitized as well as Integrated GRC Management System represent the **central nervous system of the organization**.

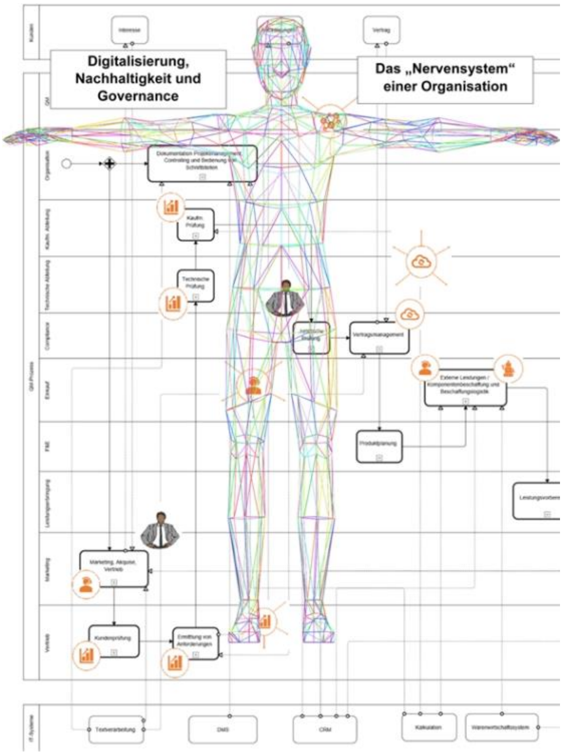


Figure 01: Digitized Integrated GRC Management System / processes as the central nervous system of an organization

It is important to ensure that digitization, sustainability and "Corporate Governance 4.0" are introduced conceptually and "holistically" into the Integrated GRC Management System.
Pure activism often leads to conflicting, non-harmonizing processes and system breaks.

Also, in order to do the right thing at the "process level", the appropriate attitude on the cognitive and emotional level is extremely important for management and employees: Tone from the top, culture, awareness, competences, motivation and much more... ("Human level")
Only then can a process organization become "effective" ("lived").[45]

Step 2: Derivation of top goals, strategies and drivers for resilience and future viability via "materiality analysis" and "management approach”

The focus of corporate action is the achievement of goals.

[44] Cf. *Scherer*, Resilienz und Zukunftsfähigkeit - GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de.
[45] Cf. *Scherer*, Resilienz und Zukunftsfähigkeit - GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de.

Here, a "differentiation" must be made: Due to the duty of **legality** (part of compliance), there are **mandatory goals** without discretionary / decision-making leeway. In this respect, it is only necessary to plan how these objectives are to be achieved appropriately, taking into account resources (time, money, skills, etc.). No decision is to be made on the objective itself due to the lack of leeway.

In the case of **goals to be set voluntarily**, an appropriate decision must first be made - using appropriate risk assessment methods within the framework of the Business Judgment Rule (Section 91 (1), sentence 2 AktG) - as to whether the target is to be set on a binding basis and, if so, how the target is to be achieved must be planned.

The question arises as to which top topics a company manager must / should focus on.[46]

For this purpose, the *"essential topics"* are identified annually.

The *"materiality analysis"* focuses on economic, ecological and social issues that are of interest to both the organisation and the stakeholders.

A "**management approach**" is used to ensure competitiveness and future viability. This shows the "responsibilities and regulations," "goals and key figures," and "measures (projects and initiatives) for achieving goals."

The minimum requirements of Section 267a of the German Commercial Code (HGB) are covered for the main topics. In addition, the sustainability report is prepared on the basis of the Global Reporting Initiative (GRI) standard.)[47]

The top goals developed by a *"materiality analysis"*

"1. Sustainable livelihood susion and business value enhancement",
"2. Customer and stakeholder satisfaction",
"3. Compliance and legally secure organization",
"4. (Project-related) Risk management",
"5. Strategic personnel development",
"6. Conservation of resources",
"7. Digitization and information security",
etc.
are then broken down to process goals and employee goals, in addition to the other departmental goals.

These *top goals* are usually related to many departments/processes and influence their objectives. In organizations, therefore, these cross-cutting topics are often controlled by staff offices or by means of a balanced scorecard.

Example from practice for strategy development and analysis of key objectives according to the Global Reporting Initiative (GRI) (Standard for Sustainability Reporting):

Source: STRABAG Annual Report 2018, p. 35 (available on the internet):

*"Given the **large number of topics relevant to our organization**, we would like to focus in our reporting, but also in our daily work, on **those topics that are material, taking into account, among other things, the economic, ecological and social impact of our organization, both from STRABAG's own perspective and from the perspective of our stakeholders.***

*In order to identify the **main topics,** we carry out an annual **materiality analysis,** during which we go through a multi-stage process, in whole or in part. The process includes the **involvement of internal and external stakeholders** in order to have the topics evaluated from different perspectives.*

***[...] issues that are crucial to our competitiveness and future viability, the respective managers in the Group developed a management approach**.*

*This makes clear in each case how we ensure **priority treatment in the Group (responsibilities and regulations),***

[46] Cf. *Scherer*, Resilienz und Zukunftsfähigkeit - GRC als „Klammer" diverser Management-Inseln, 9 / 2020, Risknet.de.
[47] Cf. *Scherer / Fruth / Grötsch* (Ed.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0",2021, p. 150.

> *which key performance indicators we develop as control parameters (targets and key performance indicators)*
> ***and which measures we derive to achieve our goals (projects and initiatives).***
> *The management approaches are presented in this annual report:*
>
> 1. ***Customer satisfaction***
>
> 2. ***Strategic personnel development***
>
> 3. ***Innovation***
>
> 4. ***Digitization***
>
> 5. ***Project-related risk management***
>
> 6. ***Conditions***
> ***(Occupational safety, health, human rights, equality between men and women)***
>
> 7. ***Resource management***
> ***(Energy & emissions, materials)***
>
> 8. ***Business compliance***
>
> ***These main topics listed above relate to the minimum environmental, social and employment issues, respect for human rights and the fight against corruption and bribery, as referred to in Section 267a of the UGB*** *[in Germany: Section 267 a Of-AGB – Commercial Code, note of the author],* ***respect for human rights and the fight against corruption and bribery, and from the point of view of the Executive Board, they cover the issues necessary to understand the impact of the company's activities.*** *This report is* ***based on the Global Reporting Initiative (GRI) standards. (...)"***[48]

GRC with risk and compliance management already provides valuable information when identifying and deciding on the top issues by highlighting legal requirements / limits as well as threats and opportunities.

For each of the strategic objectives outlined above, there is a suitable "management system island" that ensures the objectives are achieved. Ideally, these are brought together as an Integrated (GRC) Management System.

The importance of data, risk and compliance management methods for good business decisions is also emphasized by the new international *ISO standard* ISO ***DIS 37 000: 2020*** *for "Governance of organizations":* ***7.8 Information and decisions***[49]

> ***7.8 Data and Decisions***
>
> *"In everything the governing body does, it is obliged to make decisions.*
> *The continued viability and existence of the organisation depends on the decisions of the governing body. (...)*
>
> *Boards generally ensure that their decisions are made on the basis of sound alternatives or proven case studies (scenarios). (...)*
> *Since the primary purpose of data is to provide information for decision-making (whether by humans or through automation), its value to the organization is manifold: (...)*
>
> *The governing body should consider data as a valuable resource for decision-making.*
>
> *For most organizations, data is a strategic resource. (...)*
>
> *The increased value of the data also brings with it a potential increase in risk. (...)*
>
> *The governing body should ensure that the organisation identifies, manages, monitors and communicates the nature and scope of its data use. (...)*

[48] Cf. *Scherer / Fruth / Grötsch* (ed.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“, 2021, p. 151.

[49] Cf. ISO/TC 309/WG 1 “Guidance for the governance of organizations”, 2020, S. 34 ff.
(*Own* translation from English).

The governing body (should ensure[50]: (...)

- *the introduction of a system that guarantees, understands and pursues the rights, obligations and restrictions of data sets, e.g., obligations to protect privacy and intellectual property rights*

- *Implementation of a risk-based information security management system (ISMS) (...)*

Modeling objectives and related decision-making requirements makes oversight less complex and robust. Such modeling can strengthen immature control processes and highlight the interdependence of decision criteria, cognitive biases, groupthink, or unexpected scenarios. (...)"

Digital or semi-automated decision support with GRC and the rules of the Business Judgement Rule (91 sec. 1 sentence 2. AktG) is making its way into all industries.[51]

Step 3: Regulation of responsibilities

As in process management, the "management approach" for the respective top goals *"via RACI"* recommends the definition of responsibility for execution (Responsible), responsibility for content (Accountable), the drawing of expert knowledge (Consulted) and reporting lines (Informed).

Step 4: Identification of requirements regarding the respective top goal

Compliance management takes care of identification, evaluation and measures to meet various requirements from laws, case law, technical clauses, contracts, standards, etc. with regard to the respective top goal.

Step 5: Developing strategies / Planning

Risk: Goals and the paths (strategies) to the goal are burdened with uncertainty: Risk and opportunity management helps to take the right path with modern methods such as .B scenario analysis and bandwidth simulation.

Step 6: Derivation of projects / Measures with control and monitoring

The "lines of defense" ensure an optimized achievement of goals in the agreed projects / initiatives, especially with (project-related) risk management by controlling the uncertainties (Threats / Opportunities).

Step 7: Stakeholder communication on sustainability reporting

Stakeholders will be informed about the sustainability business report, among other things.
Little is known among decision-makers / authors of the annual reports that untruths may even be punished by criminal sanctions.[52]
In the meantime, DRS 20 demands that these reports receive relevant facts rather than meaningless phrases.

„(...) He’s tellin‘ me more and more
about some useless information (...)
I can’t get no satisfaction (...)” (Rolling Stones)

[50] Note of the author
[51] Cf. *Scherer*, Digital Decision Management, 12/2020 free download on gmrc.de / Publications
[52] Criminal offence of incorrect presentation in the management report, section 331 HGB and administrative offences pursuant to section 334 HGB

5. Impact / Performance / (Financial) Value Contributions of an Integrated GRC- / ESG- / CSR- Management System

"What did the Romans bring us?" (The Life of Brian)

Value balance: What are value drivers?

In the context of various calculation methods on the topic of "enterprise value", "value levers"[53] or "value drivers"[54] are named as factors influencing the enterprise value.
Thus, a good strategy, as well as good decision-making, financial, risk, compliance, purchasing, sales, IT, quality management, etc., push and each area can also destroy value, possibly even trigger a corporate crisis.

The measurability of intangible assets is a prerequisite for their control and monitoring ("if you can't messure it, you can't manage it").
Auditors can base the measurement of intangible assets on standards such as IDW S 5, S FAS 157 or IFRS 3.[55]

Sustainable and value-oriented investments are more in demand than ever in the financial market. Some investors only finance companies that demonstrate adequate economic indicators and meet comprehensive social and environmental criteria.[56]

- After the financial and economic crisis of 2008, the performance of companies that were strongly oriented towards sustainability was on average 15% better than in the respective sector as a whole.

- Investors in this case (rightly) relied on better crisis management capabilities and sustainable success.

- It will also be the case in and after the Corona pandemic.

- Also, with regard to government support programs for companies, not all companies will be supported according to the "watering can principle", but rather specific industries/sectors (hydrogen economy, quantum technology, artificial intelligence, ...) or demonstrably future-oriented organizations that still want to "improve" in digitalization and sustainability.

- At the same time, digitization, sustainability and GRC create transparency and structure. This ensures effectiveness and efficiency and reduces unnecessary stress.
- By digitally optimizing processes / methods, it is also possible to work in an enormously resource-saving manner:[57]

„Now give me money, that's what I want" (Beatles - Money)

Examples of automation savings in a single process:

Electronics company (approx. 11,000 employees):
26,160 h time savings per year / 784,800 € cost savings per year / approx. 66% cost savings compared to other workflow solutions

[53] Cf. *Rainer* in: Coenenberg / Salfeld (eds.), Wertorientierte Unternehmensführung: Vom Strategieentwurf zur Implementierung, 2003, p. 77.
[54] Cf. *Britzelmaier*, Wertorientierte Unternehmensführung: Kompakt-Training Praktische Betriebswirtschaft, 2nd edition, Olfert (ed.), 2009, p. 172.
[55] Cf. *Scherer*, Resilienz und Zukunftsfähigkeit - GRC als „Klammer" diverser Management-Inseln, 9 / 2020, Risknet.de
[56] Cf. *Kirchhoff* in: Gazdar, Kaevan et al. (ed.), Erfolgsfaktor Verantwortung, 2006, p. 20 and PWC, The growth of tomorrow, ESG-study, 10/2020
[57] Cf. *Scherer / Fruth / Grötsch* (Ed.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0" Resilienz und Zukunftsfähigkeit, 2021, p. 13.

Automotive OEM: approx. 1,400 h time savings per year;

Automotive OEM: 1 process pass to achieve ROI;

Automotive OEM: > 3,000 h time savings per year;

Recruitment companies: ROI reached after only 6 months[58]

Examples of efficiency gains through "Digital twins":[59]

Processes depicted as a "digital twin" can be simulated and evaluated, which enables optimal design in advance or during process changes:

- Manufacturers of industrial computer components (Siemens) increased production output on the same area to 10 times since its opening, (15 million units per year) through efficiency gains from the digital twin.

- Sports car manufacturer Maserati used the digital twin to produce a sports sedan after just 16 months instead of 30.

"G R C, I'm dynamite, ...

G R C, I'll win the fight, ..."[60]

6. There is only one problem left: How does GRC respectively ESG (CSR) become "sexy"?

„You sexy thing" (Hot Chocolate)

How do we manage to bring the new importance of GRC respectively ESG (CSR) for value contributions and achievement of goals into the minds of decision-makers and other employees?

Already at the *cognitive* level, the challenge is to allow managers and employees (behavioral economics) to understand and apply the new meaning of GRC respectively ESG (CSR).

However, even if the understanding of the benefits of GRC respectively ESG (CSR) is in the heads, on the emotional level a (ideally intrinsic) motivation must be generated to "want to practice GRC respectively ESG (CSR) as well."
How do we manage - like Tom Sawyer painting Aunt Polly's garden fence[61] - that the "flows at work" expected from GRC respectively ESG (CSR) make everyone happy to be "allowed to practice" GRC respectively ESG (CSR)?

"Sexy, what did you do with this old man?" (Marius Müller-Westernhagen)

The target group for "GRC respectively ESG (CSR) marketing" is not limited to "old managers".
The top executives of tomorrow in particular should be introduced to the new understanding of GRC respectively ESG (CSR) and management today.

[58] Info from *TIM Solutions* specific practical cases on savings by digitization (20.04.2020)
[59] *t3n*, Article „Was bedeutet digitale Transformation eigentlich konkret?" from 15.04.2019
Note: The author is currently supervising the dissertation of Rieger, Franz at the Uni-Klinik Regensburg on "Modeling and Impact Evaluation of a Digital Twin of a Process for the Treatment of Prostate Cancer."
[60] *Sebastian Scherer*, Cover-Version of *AC/DC*, TNT.
[61] Cf. *Keilen*, BMF.

7. Conclusion

"When the wind of change blows, some build walls and the other wind turbines or new goals and strategies" (Modified Chinese Proverb)

Deggendorf, 10.02.2021, Prof. Dr. Josef Scherer

About the author:

Prof. Dr. jur. Josef Scherer

Attorney at Law
Founder and Director of the International Institute for Governance, Management, Risk and Compliance Management at the Technical University of Deggendorf THD

Attorney-at-law Prof. Dr. Josef Scherer has been Professor of Corporate Law (Compliance), Risk and Crisis Management, Reorganization and Insolvency Law at the Technical University of Deggendorf since 1996. Previously, he worked as a public prosecutor at various regional courts and as a judge at the regional court in a civil chamber.

In addition to his work as senior partner of the law firm Prof. Dr. Scherer, Dr. Rieger & Mittag Partnerschaft mbB, which specializes in commercial law and governance, risk and compliance management (GRC), he prepares scientific legal opinions and acts as a judge in arbitration proceedings.

Since 2001, he has also worked as an insolvency administrator in various local court districts.
Prof. Dr. Scherer acts as compliance ombudsman and external compliance officer / quality management officer in various companies / corporations and is a sought-after speaker at management training courses in well-known companies as well as in the continuing education program of the broadcaster BR-alpha and the Virtual University of Bavaria (VHB).

In cooperation with TÜV, he designed the renowned and accredited part-time master's program in risk management and compliance management at the Technical University of Deggendorf and is active as an external expert in the (system) accreditation of continuing education programs.

Since 2012, he has headed the International Institute for Governance, Management, Risk and Compliance Management at the Deggendorf University of Applied Sciences as a competence center in his capacity as a member of the board of directors.

He has also been a member of the Advisory Board of the Institute for Risk Management and Regulation (FIRM), Frankfurt (www.firm.fm) since 2015.
Likewise since 2016, member of the DIN Standards Committee Services (Working Committee Human Resources Management NA 159-01-19 AA) for the development of ISO/DIN standards in human resources management and since 2017, member of the delegation ISO TC 309 Governance of organizations (Working Committee Governance and Compliance NA 175-00-01-AA for the development of ISO/DIN standards in the field of corporate governance, compliance and whistle blowing).

Likewise since 2016: technical leader of the "User Group Compliance" of the Energy Forums Leipzig and since 2018 member of the working group 252.07 of Austrian Standards International for the development of an ÖNORM 4900 ff. (Risk Management System Standards).

His research and activities focus on managerial liability, governance, risk and compliance management, integrated human workflow management systems and digitalization as well as contract, product liability, reorganization and insolvency law, labor law and human resource management.

Prof. Dr. Scherer is a shareholder-managing director of Governance-Solutions GmbH and a member of the supervisory board of various companies and foundations in the field of applied research and solutions/tools in GRC, digitalization and integrated workflow management systems.