Combined certification of risk and compliance – Essential evidence for sustainability management system and ESG due diligence

Josef Scherer

A few months ago, new certified (ISO) standards for risk (ÖNORM 4900 ff: 2021) and compliance (ISO 37301:2021) were introduced. Because of the legality principle and other new requirements from legislation and legal decisions, these systems are mandatory. However, at the same time they are the key pillars of sustainability (ESG/CSR), one of the current megatrends alongside increasing regulation and digitalisation. They are also the basis for ESG due diligence.

New requirements

In 2021, the certifiable standards ISO 37301 (compliance management system) and Ö-Norm 4900 ff for risk management systems came into force.

In April 2021, the European Commission published its draft Corporate Sustainability Reporting Directive (CRSD).[1] The new standards affect large companies with more than 250 employees, which in future will be required to produce sustainability reports[2].

In terms of compliance, on 18/11/2020 in the "bookseller judgement" the Federal Supreme Court determined that a company must keep itself updated on legal changes, and must evaluate and implement them appropriately: "Ignorance is no defence."[3]

Therefore it is advisable to be well informed on these new developments.

This catalogue of new[4] regulatory compliance requirements in respect of governance, sustainability and resilience at a global, European and German level may yet be extended further.

Compliance and risk as a basis for sustainability / resilience management systems

It is apparent that when it comes to sustainability (CSR/ESG), compliance and risk management in particular are the basic requirements for identifying and meeting the numerous requirements in specific areas.

Economic, social and environmental sustainability (ESG / CSR) largely includes identical requirements to governance, risk and compliance (GRC) and can generally only be effectively and efficiently controlled with an integrated management system.

Each component of governance or GRC (e.g. quality, risk or compliance management) simultaneously represents a key component of sustainability.

ESG – Due diligence

Due diligence is a "conscientious, careful assessment" that is (or should be) normally performed before purchasing an investment object, e.g. a company or an organisational unit, to identify and evaluate the risks and opportunities associated with the purchase object.

This can involve the acquisition of shares (share deal) or individual assets (patents, specialist staff, plant, goodwill etc., "asset deal").

The assessment by the buyer (buyer's due diligence) is almost mandatory as bad investments due to a lack of assessment can see those responsible on the buyer's side facing civil or criminal liability (e.g. for misappropriation of entrusted funds etc.) and other adverse outcomes (loss of reputation, dismissal etc.).

There are plenty of examples of avoidable bad investments with significant losses.[5]

Conversely, the seller (vendor's due diligence) is interested in transparency if they have "a lot of positives" to offer.

The result of the assessment influences the purchase decision (yes or no) and the price.

The classic business evaluation methods (e.g. discounted cash flow, income method etc.) do not achieve the desired results without robust due diligence results, as they aim to use past results to draw conclusions about sustainable existence and profitability in the future, which is a wholly unsuitable method in today's volatile conditions [see Scherer 2013].

In practice, financial, legal (compliance) and tax due diligence are (currently still) common.

Because of the recognition that other issues are becoming increasingly important, we are also seeing an increase in IT, HR and commercial due diligence assessments.

However, analyses of numerous insolvency proceedings and insights from risk management reveal that the causes of crises or high losses can lie in almost any conceivable internal or external event.

For this reason, since 01/01/2021 section 1 of StaRUG stipulates that directors or CEOs must operate a continuous early risk detection system.

Thus, to obtain an information basis for evaluation of the sustainable existence and profitability (risk bearing capacity and resilience) of an investment object, risk based (!) due diligence is required.

In other words, a comprehensive risk analysis determines which areas require further in-depth evaluation using traditional due diligence assessments.

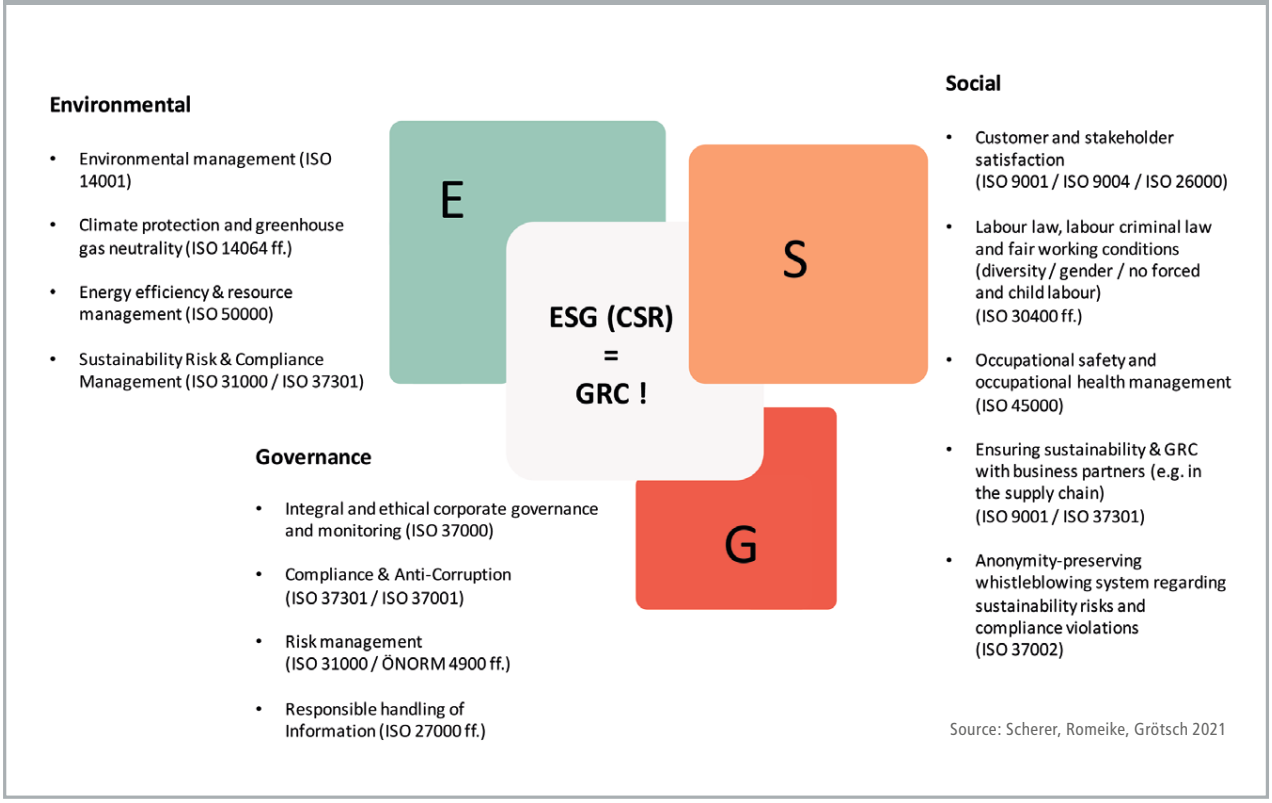
The objective of sustainability (ESG) based due diligence is not only to obtain information about risk bearing capacity, i.e. survival or resilience, and future profitability, but also to examine other economic, social and environmental sustainability factors.

The areas to be assessed as part of ESG due diligence are determined by the themes set out in various international standards (Global Reporting Initiative, Global Compact etc.) and are shown in ▶ Figure 01.

Practical relevance

Since sustainability (ESG / CSR) and digitalisation are the top two megatrends and ESG due diligence of course covers the issue of risks and opportunities in the area of digitalisation, information security and cyber security, there is a high level of demand.

Figure 01: ESG (CSR) = GRC [Source: Scherer, Romeike, Grötsch 2021]



According to Deloitte [see Deloitte 2021] 94% of institutional investors are already analysing sustainability aspects before a transaction. Of these, 30 percent change their decision about the investment after this ESG analysis. It is also notable that 54 percent of institutional players also reduce the offered price for the target based on the results of their sustainability analyses.

Efficient solution based on robust certificates

As set out above, a risk and compliance management system is the "key pillar" for a sustainability (ESG / CSR) system and for corresponding ESG due diligence, especially as it should address the areas affected by sustainability / ESG in terms of (compliance) risk identification, evaluation and management.

To the extent that certification based on the new international standards does not accept "Potemkin risk and compliance villages", i.e. "(compliance) risk accounting" that is not put into practice, but examines whether "knowledge, understanding, skills and will" exists among management and employees in respect of (compliance) risk identification, evaluation and management and whether the corresponding tools and systems are in place, presentation of appropriate (combined) certificates is an effective component of ESG due diligence.

Summary

If we compare the – less well known – specific and measurable (!) requirements from legal regulations and standards, the many overlaps between GRC and sustainability (ESG/CSR) are clearly noticeable.

This makes it vastly easier to implement a sustainability or GRC management system. Each component of GRC (stakeholder or HR management) simultaneously represents a key component of sustainability.

Compliance and risk, and corresponding technically sound certificates play an important role for each of these components and therefore also for ESG due diligence.

[1] *The CSRD replaces the Non-financial Reporting Directive. At a national level, the rules and implementation must be in place and followed in individual states for the 2023 financial year, e.g. change to the German Commercial Code for companies, banks and insurers from 01/01/2024. See CSR reporting obligations, The EU provides. requirements for future sustainability reporting., last accessed on 03/06/2021, and BMJ, Draft Corporate Sustainability Reporting Directive CSRD, last accessed on 16/08/2021.*

[2] *And turnover of over 40 million € or balance sheet total over 20 million €.*

[3] *See Beck-aktuell, No mistake of law after bribe payments for school books, 2021, last accessed on 16/08/2021*

[4] *primarily decided in 1st half of 2021*

[5] *See Hypo Alpe Adria, steel plant in South America, "Omega 55", American manufacturer of pesticides.*

[6] *German Act on the Stabilisation and Restructuring Framework for Businesses (StaRUG)*

Literature

Deloitte (2021): ESG Due Diligence als inkrementeller Bestandteil von M&A Deals [ESG due diligence as an incremental component of M&A deals], last accessed on 23/08/2021 at www.2deloitte.com

Scherer, J. (2013): Governance Management, Volume 1, 2013.

Scherer, J./Romeike, F./Grötsch, A. (2021): Unternehmensführung 4.0: CSR/ESG, GRC & Digitalisierung integrieren [Corporate governance 4.0: Integrating CSR/ESG. GRC & digitalisation], 2021, free download from www.scherer-grc.net/publikationen

Author

Prof. Dr. jur. Josef Scherer

Lawyer and former regional court judge,
International Institute for Governance, Management, Risk and Compliance Management
at the Deggendorf Institute of Technology
and member of the FIRM advisory council