

Interview

Governance, Risk and Compliance

Non-compliance destroys value contribution

RiskNET [Editor-in-chief] 23.02.2016, 17:26



A look at the media tells you a great deal about the "soul of compliance". Management misconduct is a hot topic, whether it is in the automotive sector, banking or the pharmaceutical industry. This contradicts numerous business, risk and compliance reports, which convey the feeling that everything is fine throughout the organisation. This is countered by Dr. Josef Scherer – Professor of corporate law, risk and crisis management, founder and head of the International Institute for Governance, Management, Risk and Compliance at Deggendorf Technical University – in terms of mandatory management duties in the compliance field.

Has there been an intensification of liability in recent decades? Is there empirical evidence of this?

Josef Scherer: The "perceived" intensification of liability and sanction risks for executive boards, directors, supervisory boards and even shareholders faced with the accusation of having acted in breach of their duties can be objectively measured. In the ten-year period from 1986 to 1995, there were as many judgements on manager liability as in the

previous 100 years. The number is estimated to have doubled again over the subsequent ten-year periods from 1996 to 2005 and 2006 to 2015. Because the "wind has changed" and "there are now more severe punishments for compliance breaches involving D&O insurers", officers' liability was one of the themes discussed by the commercial law department at the 70th Annual Meeting of the German Legal Association in 2014.

Lawyers including Bachmann and Bayer (the author of "Internal Liability of Limited Company Directors", GmbHR 2014, p. 897 ff.) argue that limited company directors believe they are actually exposed to huge personal risks that threaten their existence and – in fact – have much stricter liability than an executive board because directors in SMEs do not have a "comparable quality of expert advice and assistance that is now necessary to avert legally relevant breaches of care as defined by supreme court decisions. The requirements made on a director today are almost impossible to meet in practice." Even those who act largely with an awareness of their duties believe that they are threatened not only by risks under civil law but increasingly also by the possibility of criminal liability.

What is meant by a compliance-based governance or management approach?

Josef Scherer: The issue of commercial reasoning and/or decision-making and action – the focus of a great deal of business "management" or "corporate governance" literature – has for a long time had a legal basis, even if this is not conclusive and comprehensive:

There are areas where behaviour (reasoning/decision-making/action or omission) is clearly specified and there is no scope for decisions or discretion. These are known as "circumscribed actions or decisions" based on the legality principle, compliance requirements (which may go even further due to self-imposed obligations), a "reduction of discretion to 0" (for decisions with certain expectations or if any reasonable and conscientious decision-maker would only decide in one direction). Any differing behaviour would be a breach of duty and thus represent significant grounds for liability or sanction.

In areas with scope for discretion, the legislature and the judiciary have already defined numerous explicit rules for compliant behaviour by managers. It is important here to highlight behaviours associated with reasoning as a process to be completed prior to decisions. With regard to "commercial decisions" (§ 93 Para. 1, section 2 AktG), reasoning has a lot to do with information management and psychology (prevention of cognitive distortions and external manipulation) and, as an important element of management duties in directing the company, is subject to the imperative of "propriety

and conscientiousness", i.e. not arbitrariness but legal verifiability. Likewise, decision-making in the interests of the company (after mandatory consideration based on appropriate (sufficient for the objective) information) has to be fully legally recognised by the courts in their decisions and judgements.

If mandatory behaviour were not to be performed or not in the correct time frame and form, this would represent a breach of duty subject to liability (compliance violation), in some cases also under criminal law. This is what is known as the "legality obligation" of management, which applies in both public and civil (or criminal) law.

In the context of liability, what role is played by the due diligence of a conscientious businessman?

Josef Scherer: It is important to always consider the general clauses, which state that an executive board, supervisory board or director must behave like a "conscientious businessman". For supervisory board members § 116 AktG refers to § 93 AktG. Directions, contractual obligations etc. can turn what is actually a discretionary duty into a mandatory duty.

Legal requirements and judgements from individual cases that specify what is meant by "conscientious corporate management" can be found in all areas of a company, for example in sales, anti-corruption law, labour law, international trade law, money laundering law, intellectual property law (trademarks, patent law, licensing law), trade law, cartel law, product safety and liability law, tax law, transport law/logistics law, contract law, advertising law, competition law and customs law. This results in a range of mandatory requirements for the relevant process steps derived from laws/regulations and also from individual case judgements (for example the recent Federal Supreme Court (BGH) judgement on organisation to prevent liability for unfair competition).

Ideally, the procedural documentation in the relevant areas contains the applicable requirements and tools (sample documents, IT tools, checklists) to meet these requirements. This enables the abstract and supposedly unmanageable legal rules to be incorporated into concentrated and specific processes – this is how compliance works in practice.

Violation of the "recognised academic and professional standards and knowledge" in terms of proper corporate management and governance is another kind of behaviour in breach of duty. But what exactly is meant by "recognised academic and professional standards and knowledge" in this context?

Josef Scherer: What the latest academic and professional standards and knowledge actually means in a specific situation has only been stipulated in very rare cases in legislation or case law. The "recognised academic and professional standards and knowledge" in terms of the level of development of rules, characteristics, behaviours, methods, tools, management systems etc. associated with corporate management and governance are defined as "predominant recognition by prevailing academic opinion as theoretically correct and by the prevailing opinion of relevant practitioners as proven".

For example, we would have to ask whether recognised (international) standards (for example ISO 31000:2008 (risk management), ISO 19600:2014 (compliance management) or COSO I:2014 (internal control), IDW PS 980:2011 (principles of proper auditing of compliance management systems) or COSO II:2004 (ERM)) represent what is known as "anticipated expert opinion" or whether in case of a dispute on this issue the judge should commission a separate expert report to establish the facts. According to the Federal Supreme Court and the Federal Administrative Court, established standards can ideally be presumed to reflect "recognised academic and professional standards and knowledge". However, these may frequently be lacking. In some areas, standards lag behind this "recognised level" of "prevailing opinion" among academics and professionals – in other words, the professionals are often way ahead.

It is also important to be aware that adherence to the "recognised academic and professional standards" – including in terms of risk and compliance management – does not involve any (!) scope for discretion. It represents a minimum requirement and provides a yardstick for assessing fulfilment or breach of duty. However, how this is achieved is not definitively stated. As the saying goes, "All roads lead to Rome" – in other words, the specific methods to be used are not stipulated. But they must be appropriate methods.

To the extent that specific actions are not stipulated, there is a possibility of discretion for management. If there is some discretion, § 93 Para. 1 p. 1 of German Company Law (AktG) states a long recognised general principle. If a manager in a specific situation is faced with a decision subject to uncertain expectations or risk, and there is a complete ruling on that situation in existing judicature or case law, he is bound by that ruling.

Otherwise, his only obligation under the law is to apply an appropriate management decision-making method to ensure that the situation does not constitute a breach of duty – this is known as the Business Judgement Rule.

That's a nice title. But what specific things have to be taken into account when using the Business Judgement Rule?

Josef Scherer: This is where a further area for risk, opportunity and compliance management can be found. In terms of information acquisition and evaluation within the scope of the Business Judgement Rule, recognised methods of risk and compliance management help to delineate the fiduciary duties associated with possible actions and, in terms of the risks involved, to prevent acting "on gut instinct". Recognised standards are already in place in this area.

Risk management creates transparency in respect of decision-making based on the requirements of the Business Judgement Rule and sets out some key principles: consideration of risks and benefits, and of the company's risk bearing capacity.

Following the above thesis, a manager is not acting in compliance with their duties if – as frequently happens in practice – they have significant shortcomings in their level of business management knowledge and skills, have not delegated and the company suffers losses as a result of incorrect commercial decisions.

What is the relevance of standards? Do they provide a guarantee that recognised academic and professional knowledge will be applied?

Josef Scherer: In some circumstances "standards" may reflect the "recognised academic and professional knowledge". However, this has to be verified in each individual case. Under the German constitution there are only three powers: the legislature, the judiciary and the executive. Experts are not included. As the requirements, regulations and sets of rules referred to below as "standards" (for example DIN / ISO 9001:2015 for quality management, one of the most widespread and most frequently certified standards, but also DIS/ISO 19600:2014 / IDW PS 980:2011 for compliance management or the new OECD Principles of Corporate Governance 2015) are issued not by official bodies but by "expert committees" organised under private law (DIN/ISO/VDI/VDE/IDW/OECD etc.), standards are not normally legitimised by one of the three powers. Therefore, they do not represent legal norms. Likewise, they cannot be used as rules of interpretation for legislators or legal judgements, as the legislature or judiciary may not be subject to any influence by private institutions. This is why they are not used as "voluntary self-commitment" by the courts either.

They have absolutely no obligation to allow their judgements to be influenced by the requirements in standards. Summary: Experts only act as advisors to enhance the specialist knowledge of the legislature, judiciary and executive. Under some circumstances, "standards" can be viewed as "anticipated expert opinion".

Why are we still seeing such serious compliance violations by managers?

Josef Scherer: Failure to take the issue seriously, naivety or ignorance can all be causes of violations. Better awareness and appropriate management training in the areas of governance, risk and compliance could have a big impact. There is a huge deficiency in basic GRC knowledge among decision-makers.

Basic management training courses lack technical, legal and commercial content, particularly the importance of an interdisciplinary approach. And this is exactly what would help to make managers leaders in the compliance field again.

Where do you believe is there the greatest need for action in research, teaching and training when it comes to compliance and GRC?

Josef Scherer: There are numerous (research) activities in the field of governance and compliance that are necessary to create transparency, clarity and security in managers and supervisory bodies about their obligation to do the right thing (to manage and govern companies properly):

1. The search for a globally applicable common denominator for value and rights systems and transparency on key differing approaches (see G20/OECD Principles of Corporate Governance, 11/2015);
2. Effective incentives for "reasonable" behaviour and the required political and economic conditions;
3. Linking Industry 4.0 with GRC processes;
4. Integrative, interdisciplinary GRC management systems;
5. Adaptation of training systems to the requirements of future GRC models;
6. Global understanding, uniform communication and standardisation approaches in terms of GRC;
7. Proof and measurement of the dependency on GRC maturity on the one hand and the level of compliance, value contribution, sustainability, and achievement of objectives on the other.

These are just a few examples of research themes for the coming years.

Calculation of financial value contributions for proper, standard-based corporate management and governance generally or in individual disciplines, taking into account maturity and compliance, would significantly increase openness to reasonable and legally-compliant behaviour, while simultaneously making things that destroy value contribution more transparent. If the state and its three powers were also to focus on these results, we could even hope to eliminate the intransparency of arbitrary action through unnecessary regulation and bureaucracy.

Since 1996, **Prof. Josef Scherer** has been professor of corporate law (compliance) at Deggendorf Technical University specialising in risk and crisis management, restructuring and insolvency law, and is the founder and head of the International Institute for Governance, Management, Risk and Compliance Management at Deggendorf Technical University (THD). He previously worked as a public prosecutor and judge in the civil division at various state courts.

In addition to his work as a senior partner at the commercial law firm Prof. Dr. Scherer, Dr. Rieger & Partner, which specialises in governance, risk and compliance (GRC), he produces academic legal reports and acts as a judge in courts of arbitration. From 2001 to 2014, he also worked as an insolvency administrator in various municipal court districts. In conjunction with the TÜV Süd and the RiskNET competence portal, he designed the accredited part time Masters course in risk management and compliance management at Deggendorf Technical University, and is the course leader and lecturer. His research, current work and numerous publications are in the areas of management liability, governance, compliance and risk management, contract management, product liability law, and crisis, restructuring and insolvency law.



[Interview conducted by Frank Romeike, editor in chief RiskNET and board member at the Institute of Risk Management and Regulation; The interview was originally published in issue 02/2016 of the magazine RISK MANAGER.]

[Source of images: © Sven Hoppe - Fotolia.com]

