RiskNET®

Interview

Risk Management and Corporate Governance

Compliance risk analysis

RiskNET [Editor-in-chief] 22.04.2015, 17:16

Compliance and risk analysis: How do the two issues fit together? The concept of compliance includes adherence to, observance of and conformity to particular instructions. In addition to an organisation behaving in a way that adheres to legal standards, the aim of an effective compliance organisation also involves observance of internal company requirements (such as a code of conduct), to reduce or even prevent liability claims or other legal detriments for the company, its institutions and employees. In some cases there is a narrower view that it only involves avoidance of obligations punishable by fines or financial penalties.

Consequently, compliance requires an appropriate risk management system and risk analysis for the relevant compliance risks and evaluation of the risks resulting from non-compliance. Thus, there is essentially no significant difference between compliance risks and other business risks. In terms of legal liability, corporate compliance creates a link to risk management and is a part of risk management and appropriate corporate governance. **We spoke to Prof. Josef Scherer, International Institute of Governance, Management, Risk and Compliance Management at Deggendorf Technical University, about the latest developments in the area of compliance and corporate governance.**

The former and now late Financial Director Heinz-Joachim Neubürger was unable to agree a compromise with Siemens and was therefore ordered to pay a fine of 15 Million EUR in damages by the Munich State Court. In their explanation, the judges outlined the fact that setting up an inadequate compliance system, failing to monitor it sufficiently, and inadequate compliance risk analysis represent a clear breach of an executive board's duties. How do you assess this judgement from a compliance risk analysis perspective?

Josef Scherer: The judgement doesn't actually contain very much that's new and is not really a major surprise, given that numerous previous judgements relating to legally compliant business organisation went in a similar direction. However, the details of the judgement are interesting. They reiterate a lot of familiar guidelines for managers, supervisory board members and compliance officers.

For example, we can read that setting up a functioning compliance management system is mandatory and is not a matter of discretion. There is scope when it comes to the actual design of the system. But it is important that the aim of ensuring legal compliance is achieved. It's all a question of appropriateness. The explanation is also worth reading for what it says about the principles of proper corporate management and monitoring – in other words good governance – and about process management and proof. The burden of proof mainly falls on the manager. Even if it is unclear whether the possible breach of duty caused the losses in question, the executive board or directors must clear their name. At numerous points, the duty to carry out conscientious corporate management and monitoring with no scope at all for discretion is emphasised. Other important points are: When there are alarm signals, an appropriate (effective) response is required. Clear, documented rules of responsibility are essential, and responsible employees must be provided with appropriate resources and know-how.

The executive board or directors must obtain information themselves and monitor any delegated activities. If there is resistance within the team, the supervisory board can be brought in as an emergency measure. The supervisory board also has its own duty to monitor whether a compliance management system is in place, and to ensure that it is followed and functions effectively. The compliance management system must reflect recognised academic and professional standards and knowledge. If there is a breach of the duties outlined, even ordinary negligence is sufficient for a director or executive board member to be personally liable to pay damages under civil law.

The supervisory board and/or shareholders even have a duty to sue the executive board or directors for damages if they have breached their duty. It's not enough to do something, you have to do the right thing and do it correctly.

What 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, either in legislation or case law. 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. 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. However, 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 what is known as the Business Judgement Rule.

Do industry-specific regulatory "standards" (such as the minimum requirements for risk management as administrative instructions published as a bulletin by the Federal Financial Supervisory Authority, or official statements by the ECB) count as "recognised academic and professional standards"?

Josef Scherer: As lawyers like to answer: that depends. If MaRisk were to reflect current prevailing academic and professional opinion, the answer would be yes. However, from a subjective point of view I tend to assume that these minimum requirements are already lagging well behind the prevailing opinion, and so I would answer no to your question.

Why is the Business Judgement Rule almost unknown in practice?

Josef Scherer: The Business Judgement Rule as stated in law is rarely discussed as a decision-making method in business management literature or teaching, if at all. For example, the 25th edition of the standard work "Allgemeine Betriebswirtschaftslehre (General business management)" by Wöhe published in 2013 contains a lot of information about making decisions in the face of risk and uncertain expectations. But there is no mention of the Business Judgement Rule.

It is evident that professionals need to take a more comprehensive approach. Any manager faced with risk or uncertainty who bases his decisions on business management literature alone and fails to apply the Business Judgement Rule due to a lack of explanation or knowledge, is acting in a way that may be illegal and is highly risky from a personal point of view. The situation is similar regarding the principles of a legally compliant organisation, which have formed part of the legal framework for some time now. Examples like these are numerous. You could definitely put forward the provocative thesis that, on issues that now incorporate a great deal of case law and legislation (corporate compliance), there are areas where business management teaching has been overtaken or may even be incomplete or incorrect.

What does application of the Business Judgement Rule mean in real terms – for example for a bank's executive board?

Josef Scherer: In terms of the Business Judgement Rule, a manager faced with a decision has to consider the following points: 1. Analysis of required information, collection of appropriate information and evaluation of that information; 2. Appropriate weighing-up of the evaluated information; 3. The decision must be made in the company's interests.

The decision should be documented and may not be unreasonable (see § 93 Para.1 p.2 of German Companies Act (AktG)).

In this context, it is important to note that § 93 Para. 1 p. 2 of the German Companies Act (AktG) represents only a privilege and rules out a breach of duty in civil and criminal law if the method is applied correctly.

Improper application of the Business Judgement Rule therefore results in liability for the result of the decision implemented, if correct application of the Business Judgement Rule would have led to a measure not having been taken and therefore the loss having been prevented.

By contrast, there is no liability if the loss would have occurred even with a correct decision or in any event (lawful alternative behaviour). In other words, within the discretion granted to entrepreneurs, there is no obligation to implement successful decision and actions, and decisions with a negative or even very expensive outcome are tolerated, provided the correct methodology has been appropriately applied.

What are the rules for the burden of proof?

Josef Scherer: In criminal law, the principle of "in dubio pro reo" (when in doubt, for the accused) applies. The investigating authority must conduct objective investigations and ultimately, the judge making the decision must be convinced that the evidence presented satisfies all of the subjective and objective legal prerequisites. The accused does not have to prove his innocence.

By contrast, in civil law the principle applied is that the plaintiff must prove all the necessary prerequisites forming the basis of the complaint. However, there are numerous exceptions and exceptional rules in laws. For example, in terms of proper and conscientious business management in compliance with § 93 Para. 2, p.2 of the German Companies Act (AktG), the executive board must be able to prove dutiful and blameless action.

How can an executive board involved in a decision-making process assess whether they are exposed to an increased risk of personal liability?

Josef Scherer: In addition to the company's risk bearing capacity, the risk bearing capacity of the manager should never be exceeded. A manager needs good advisors in advance. Once losses have been incurred, there is not much assistance that even the best lawyers can offer.

The question of the relevance of corporate risks in terms of their impact on the personal responsibility of management is not easy to answer and – as far as we can tell – is not an issue that is being fundamentally addressed by academics or professionals. We can get close to an answer by evaluating responsibility (list of duties) for personal and external action (or omission) across case groups or by addressing the issue of "personal risk bearing capacity". In parallel to the risk analysis levels for companies, additional personal escalation levels could be set up for manager liability, in order to achieve a higher level of awareness. These escalation levels could be defined using the following structure:

Highest priority: Risk of death or injury, personal or external. Justification for highest priority: Including ethical reasons and uninsurable risks under criminal law.

Medium priority level: Increased financial risk not covered by D&O insurance, which significantly jeopardises or exceeds the personal financial circumstances.

Lower risk level: Risk to own position and reputation due to responsibility for damage caused by the company.

In this context, it is useful to know that there are some areas that cannot be delegated and some delegations that were originally effective become ineffective in crisis situations. Situations that are relevant in terms of management liability can happen suddenly or be caused by creeping developments. In many cases, management errors accumulate and eventually lead to a situation that results in management liability. Sudden events should be reduced to those that are unavoidable through prophylactic risk management. Creeping developments can be effectively identified by "risks of changes" management and regular self-audits (managers' MOT) and require prompt action. Similar to product monitoring, when it comes to management liability issues it is important to implement a continuous monitoring system.

In a company it is important not only to expand the value drivers but also to identify, evaluate and manage weaknesses at an early stage. Where management remains inactive or depends on gut feeling alone and the company loses value and stability due to negative results, the following question has to be asked: In terms of prudent and conscientious management, does management have a liability and a duty to be aware of and to (reasonably) apply recognised tools and methods from law, technology and business and to prevent loss situations and crises? This question can be answered in the affirmative.

Since 1996, Prof. Josef Scherer has been professor of corporate law (compliance) at the Technical University of Deggendorf, specialising in risk and crisis management, restructuring and insolvency law, and is the founder and head of the International Institution for Governance, Management, Risk and Compliance Management at the Technical University of Deggendorf (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 and RiskNET he designed the accredited part time Masters course in risk management and compliance management at the Technical University of Deggendorf, 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.