

## TECHNOLOGY RISK MANAGEMENT AS PART OF CORPORATE GOVERNANCE: THE ROLE OF THE BOARD DIRECTORS

**Reference is always being made to the role of the BoD (BoD) in matters of technology risk management and IT security. But what role should the directors play in such matters, or more specifically – how can the board become usefully and productively active?**

Dr. Bruno Wildhaber LL.D., CISA, CISM, CGEIT

Demands on the BoD have without doubt dramatically increased in the past few years. At the present time, even 'professional' board members scarcely dare to serve on more than three to five boards at once<sup>1</sup>.

This can be explained by the fact that pressures placed on board members have massively increased due to extensions to their areas of activity, as a result of the inherent responsibility perceived by the board as such, from the legislative aspect, from the viewpoint of the stock- or shareholders, as well as from the public at large and from the media. Board members today have to concern themselves more intensively and in detail with the business and its management. The board is thus not only to administer a corporate entity but also to lend active entrepreneurial and constructive support to management. The board can only then provide entrepreneurial advisories when it commits itself entirely to the overall corporate interests of a business and its stock- or shareholders.

In this regard, we already find ourselves in the area of corporate governance, which requires that a business be managed in an integral-, strategy-oriented-, controlled and situational manner:

- Integrated: Integration of the different business disciplines and organisational units;
- Situational: Situational acting must still be possible, no stubborn acceptance of so called "best practice", focus on optimised, stakeholder oriented practice;
- Strategic: All activities must be in line with the corporate strategy;
- Controlled: A control system needs to be established which allows for a balanced risk management; and last but not least

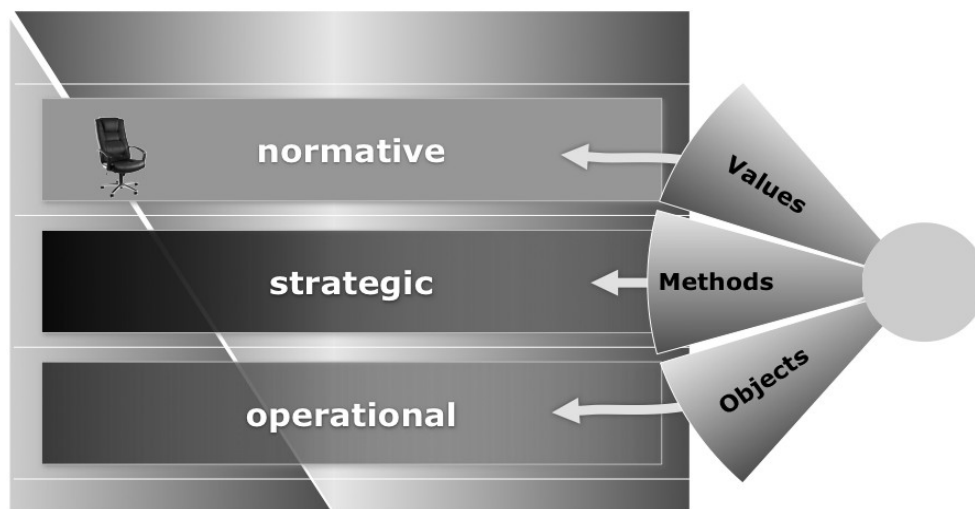
---

<sup>1</sup> Situation as seen from a Swiss perspective, however, most statements in this article can be transferred to most countries and organisations.

- Interdisciplinary thinking and communication.

## Legal Background

The role of the BoD varies from country to country. However, to manage risk is on the list of all supervisory bodies. The supreme administrative body of a corporate entity in Switzerland is the BoD, as laid down in the Swiss Federal Obligations Act. Generically, the structure of the decision latter of an organisation can be drafted as follows:

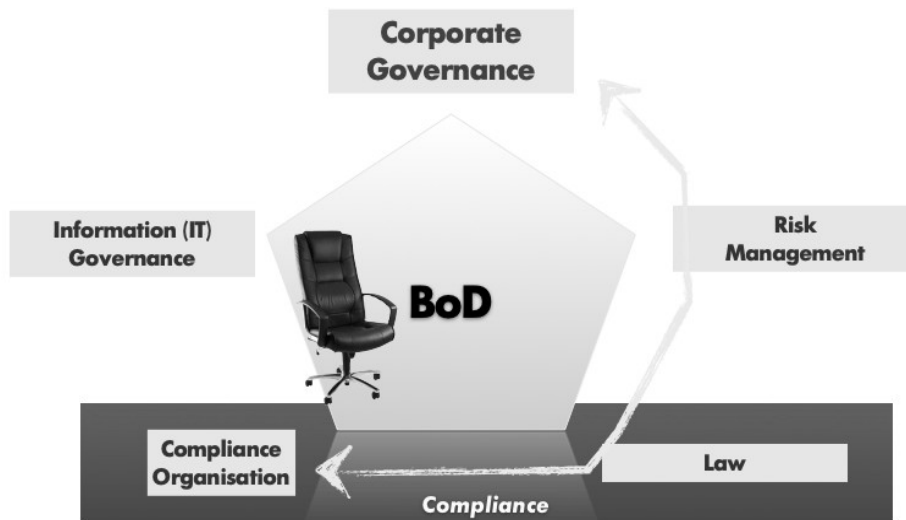


At the normative level, this means that a BoD is, among other things to issue organisational regulations and set up additional infrastructural bodies, for example the audit committee<sup>1</sup>. Added to these, are responsibilities in connection with risk management and the introduction of an 'ICS' - internal control system. Infrastructures and procedures are therefore required to permit the risks of the business to be assessed and addressed. It is not coincidental, that compliance includes the discipline of risk management as its central building block. In recent terminology, this discipline is often referred to as 'GRC' - governance risk compliance.

---

<sup>1</sup> The competence of the BoD varies, check national legislation. For an overview of governance concepts see Hilb, p. 21.

The disciplines which make up GRC can be depicted as follows:



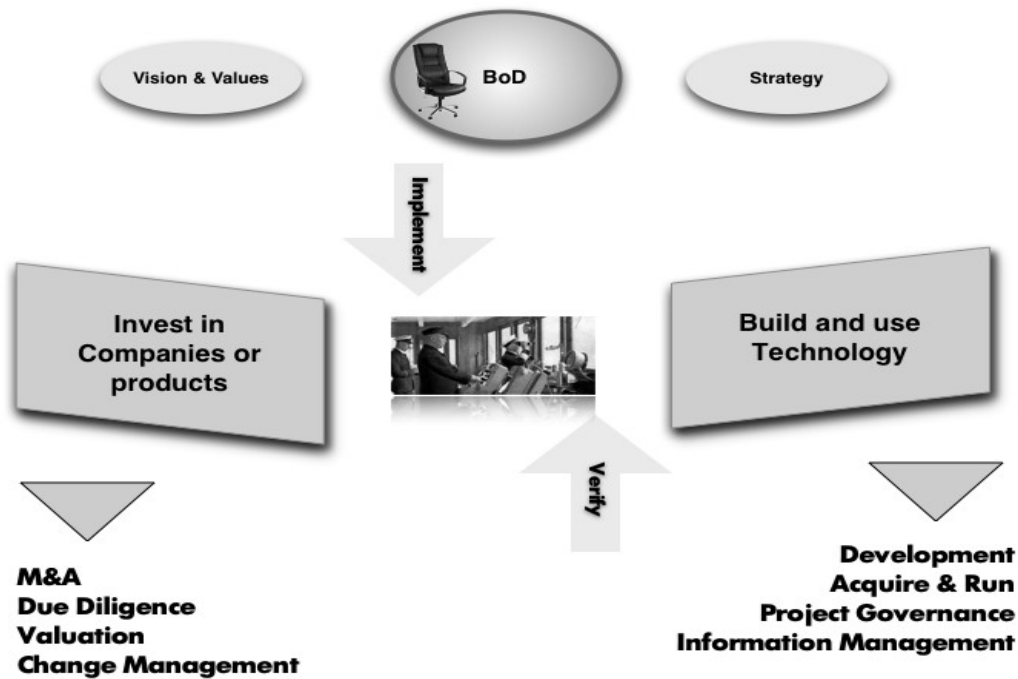
No this is the theory, but how are technology risks handled in practice? One would expect, that the BoD receives and manages a list of company relevant risks, providing a comprehensive risk summary. The focus should be on the normative and strategic level, where risks can affect the enterprise on a long-term basis.

### **Risk Management Reality**

Although the information system for the BoD is becoming all the more refined, it is rather more improbable, that risks are specifically highlighted; at best there is probably a special committee of the board to occupy itself with such matters. Modern reporting includes reports from the chief executive officer and the chief financial officer, including current charts, to include the current financial position as well as a schedule of the more important projects, but scarcely specific risk reporting.

### **Technology Risk – it is an investment**

How should the BoD address technology risks? Primarily, the BoD is managing investments in different phases, from the development to the expensive operational phase. Basically, investments can be broken down into two classes: Invest in companies or products or build and use technology.



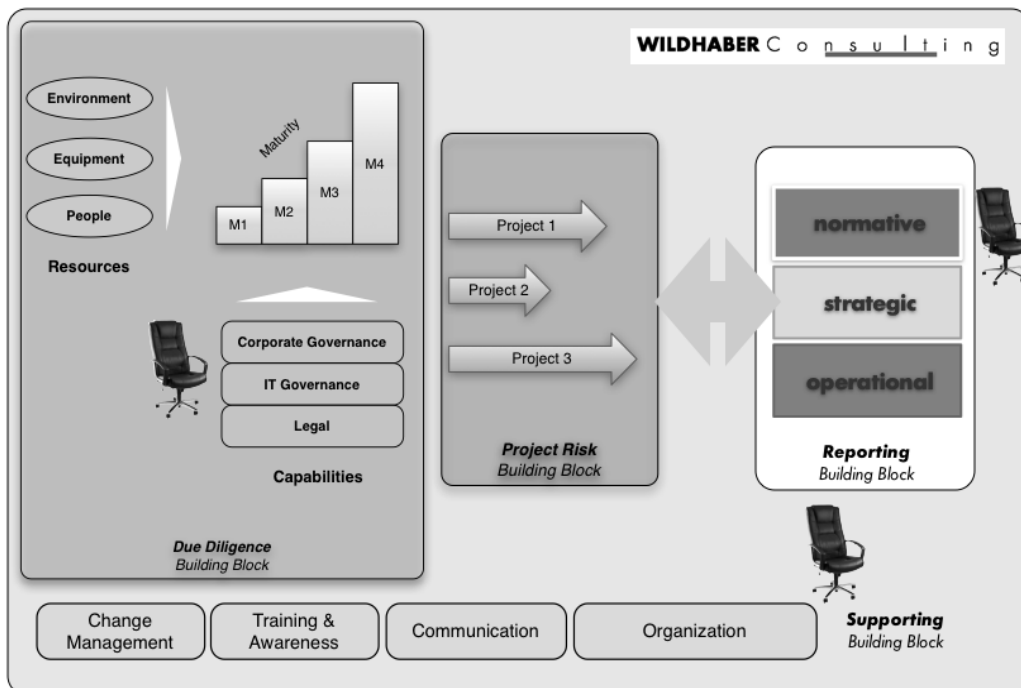
What does this now mean for addressing of technology risks? In normal cases, the BoD will only be confronted with matters of technologies, when larger capital investment is to be entertained, either to complete a larger project or to takeover a (technology) enterprise (merger and acquisition). The BoD has thus to take decisions on business with which it has little or no relation. This, as a rule leads to a resolution being passed by the board to entertain an overall capital investment, but the implementation of the project is then not further accompanied by the board. The BoD thus assumes that the strategic management level has the capital investment 'under control'.

Under certain circumstances, risks are shifted by retaining a general contractor to carry out the realisation process and to address the problem solution itself. This only has the effect of covering up the potential risk for the BoD, indeed it is to be feared, that the real problems only appear when the project has been in imbalance over a longer period of time. This signifies for boards of directors, that regular and detailed information on risks has to be insisted upon in cases of larger capital investment or projects. Management should build-up a system to collate product- and project risks in order to illustrate actual risk situations transparently at all times. It is of decisive importance in this regard, to provide a simple illustration of the risks involved. A graph showing the five main risks should suffice. In this respect, risks should be illustrated not only with reference to the current point in time, but also within the scope of the historic development. It is often forgotten, that many risks, which later appear in the course of a project, were already previously assessed but no counteractive problem solution was pursued.

## Operational Risk

The implementation of countermeasures against operational risks is something of a more serious nature. These types of risks are to be taken into consideration in the build-up of an internal control system. The BoD is entitled to expect, that technologies are operated after the state-of-the-art, meaning with the necessary due care and according to valid principles of proper correctness. In this regard, attention is drawn to the report of the auditors and also possibly to that of the audit committee. In practise however, it has been shown, that the addressing of risks is not sufficiently targeted. An enterprise should continuously improve its capabilities and work with maturity models for the measuring of due compliance dates. From the elaboration aspect however, the already numerous existent guideline frameworks and standards serve as a help. In practise however, it has always been shown, that much too much emphasis is placed upon prevention. This means that attempts are made to describe all manner of conceivable, meaningful and meaningless threat scenarios, and the exercise of a consistent and targetable monitoring activity is forgotten. Or, to put it another way, elementary monitoring is ignored in the face of full confidence in preventive regulations. With regard to large projects, it is however indispensable to be able to ascertain at all times what real status of results has been achieved.

A comprehensive Risk Management model will include:



## IT - Security

What affect does the foregoing actually have on IT security? IT security has no claim to special treatment, as it is always a part of an overall risk appreciation. The most important task in operative IT security is the consistent monitoring of weak points and structured communication to all the competent corporate bodies. Should risks accumulate, then it is absolutely conceivable, that these are communicated to the BoD, whereby an overall assessment of the entire risk situation should also be given. Should the BoD ignore technology risks and should it not be prepared to setup the necessary infrastructure, then it will scarcely be possible for the strategic and operative level of management to achieve satisfactory results. Should readiness to act be absent, in the face of evidentially high risks, then those with managerial responsibility have no other choice than to ascertain the risk extent themselves or to call upon the assistance of the corporate auditors.

*'The most important task, within the scope of operative IT security, consists in the systematic monitoring of weak points and of structured communication to the competent corporate bodies.'*

### **'Nose In – Hands Out'**

The BoD must therefore be aware of the role that information plays in the business and should then bring up the technology risk for discussion when this exercises great influence on the risk position of the enterprise. In the majority of boards of directors, such risks should only be brought up for discussion when notable proportions of the capital investment are entertained in large technology undertakings. So that the BoD can address technology matters efficiently and meaningfully, clear competence demarcations should exist and structured decision-taking processes be described. In addition, reporting infrastructures should exist in order to permit the BoD to obtain a clear picture of the current status of any undertaking. Transparent illustrations should show the financial- as well as the contentual targets and the degree of targeted achievement. Furthermore, a risk graph will be required illustrating the actual project risks and their significance as well as to illustrate risk potential. The BoD should proceed on the basis of 'nose in – hands out' and request regular information, but not directly interfere in operating activities, but be indirectly active via the described internal organisation.

*Recommended reading:*

*New Corporate Governance: Successful Board Management Tools, Martin Hilb, 2008,  
ISBN 978-3540687177*

Wildhaber Consulting  
Postfach 115  
CH 8603 Schwerzenbach  
Switzerland

Tel. +41 44 826 21 21  
Fax. +41 44 825 31 60

[info@wildhaber.com](mailto:info@wildhaber.com) / [www.wildhaber.com](http://www.wildhaber.com)