Michael Dobler

Auditing Corporate Risk Management
– A Critical Analysis of a German Particularity –

2001-03

(First Draft: July 2001)

Revised Version: November 2003

Auditing Corporate Risk Management
– A Critical Analysis of a German Particularity –

by Dipl.-Kfm. *Michael Dobler*, MBR
(Ludwig-Maximilians-University Munich)

Abstract

In 1998, the German legislator obliged public limited companies to install a system to detect risks endangering corporate going concern at an early stage. Moreover, he required the auditor of annual financial statements to audit this risk monitoring system. This task is an international novelty forestalling the Sarbanes-Oxley Act. To contribute to the emerging international concern from a German point of view, I discuss the legal and the professional approaches to auditing corporate risk management. Highlighting specific legal and factual limitations and using empirical data from audit opinions of German companies listed in the DAX 100, I investigate the impact of the new audit obligation on the expectation gap in auditing. The results suggest doubts whether the auditors will fulfil the supervisory board's needs or the public expectations in auditing. At least, reporting on the audit shows deficits in both regulation and practice.

Keywords: auditing; audit opinion; expectation gap; internal control; risk early recognition system; risk management; risk reporting; Sarbanes-Oxley-Act; test of controls.

JEL Classification: G30; G39; M40; M49.

Acknowledgement

This paper is a revised version of my paper „Auditing Risk Management – A Critical Analysis of a German Particularity" presented at the First European Auditing Research Network Symposium (EARNet) held in Wuppertal in October 2001. I thank the participants of the symposium session chaired by *Christopher Humphrey* as well as *Wolfgang Ballwieser*, *Bernd Hacker*, *Silvia Hettich*, and *Werner Rockel* for helpful comments.

1. Introduction

For the last decade, corporate governance and internal control have gained increasing interest internationally. Prominent corporate crises and failures gave rise to severe public criticism on corporate governance in general, and on corporate risk management and risk reporting in particular.[1] The German legislator responded to this animadversion by passing the Law of Corporate Control and Transparency (*Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, KonTraG*) in 1998. This legislation obliges the management board of a public limited company (*Aktiengesellschaft*) to set up a risk early recognition system (AktG § 91, para. 2). Furthermore, incorporated companies which are at least medium-sized and groups have to report on the risks of the future development (HGB §§ 289, para. 1, clause 2; and 315, para. 1, clause 2).[2]

Both requirements merely have declarative character, because they substantiate the managing board's general duties of care and control[3] and the existing requirement to disclose information on the business situation and its anticipated development.[4] These demands are associated with corresponding audit requirements. The explicit requirement of auditing the risk report derives from the general liability to audit the management report (HGB § 317, para. 2, sent. 2) and may be seen as a redundancy.[5] However, the requirement to audit the risk early recognition system is a novelty in Germany and a forerunner internationally. The auditor of a public limited company has to assess

(1) whether the managing board has taken appropriate measures to install a risk early recognition system pursuant to AktG § 91, para. 2;
(2) whether these measures are appropriate for their purpose; and
(3) whether the monitoring system is able to perform its task (HGB § 317, para. 4).

Hereby, vagueness arises because the legislator does specify neither the risk early recognition system nor the audit procedures. Moreover, the auditor cannot revert to pertinent international standards on auditing. Recently, the Sarbanes-Oxley Act of 2002 introduced alike duties by requiring internal controls and the disclosure of the management's assertion of internal controls which are subject to an audit.[6] Due to obvious similarities, the German forerunner experiences may provide guidance for standard-setters and practitioners internationally.

The specific German requirement to audit the risk early recognition system results in the following problems, which will be investigated in this paper and which are to be discussed even beyond the Sarbanes-Oxley Act and the corresponding *SEC*-Rules:

(1) What demands are made on the risk early recognition system and the risk report? And what function is assigned to German auditors in supervising corporate risk management?
(2) How shall auditors proceed to fulfil the legal requirements? What specific limitations does the auditor face?
(3) In how far may this audit actually serve the supervision and transparency of corporate risk management and thus help in reducing the expectation gap in auditing? What conclusions arise from recent empirical findings?

---

1 See *Solomon/Solomon/Norton/Joseph* (2000), p. 448.
2 The same regulation applies to registered co-operatives among others.
3 See AktG §§ 76, para. 1; and 93, para. 1, sent. 1; *Hommelhoff/Mattheus* (1998), p. 251.
4 See *Baetge/Schulze* (1998), p. 940.
5 See *Moxter* (1997), p. 724.
6 In particular, see Sec. 301 (2)(A); 302(a)(4)(B); and 404 of the Sarbanes-Oxley Act, which is available at: http://www.aicpa.org/sarbanes/index.asp. For a discussion see e.g., *McConnell/Banks* (2003).

The paper is based on an overview of requirements arising from both legislation and standards of the German auditing profession. These are discussed first from the audit point of view and second respecting to the expectation gap in auditing. Besides a critical reflection of literature on auditing the risk early recognition system, this investigation emphasises coherence with other audit requirements and provides empirical evidence from audit opinions of German DAX 100 companies. Although I refer to the German setting, the results may fertilise the emerging international discussion of audit requirements referring to corporate risk management.

2. Legal Requirements to Risk Management and Auditing in Germany

2.1. Risk Early Recognition System and Risk Reporting

The term "risk" is interpreted unevenly in common usage and academic literature. An applicable view is provided by *Helten*, who defines risk as lack of information on achieving aimed objectives.[7] This definition consists of the components "information deficit" and "target aiming". The information deficit results from the indeterminacy of components of cause and effect relations. Target aiming is essential for the analysis of economic behaviour, as succeeding or missing targets assumes one or more fixed objective(s).[8] Risk may be classified in risk in the broader or narrower sense by the direction of ex post deviation from a set target. Risk in the broader sense is the general possibility of deviation from the target, whereas risk in the narrower sense just covers potentially negative deviations. Without doubt, the legal term risk according to the Law of Corporate Control and Transparency solely aims at risks in the narrower sense.[9] These risks shall be material by means of endangering the going concern or impairing the net worth, financial position and results of the enterprise in a sustainable manner.[10]

Risk management serves assuring the continuation of the corporation as a going concern. Risk management is a continuous process: risks are identified, analysed and evaluated (risk early detection); based upon the gathered information, measures of risk policy are chosen and implemented, and their actual effects are controlled.[11] AktG § 91, para. 2 obliges the managing board of a public limited company „to take suitable measures, particularly by establishing a monitoring system for early recognising developments which might endanger the company as a going concern." As risk handling remains unconsidered, solely a risk early recognition system and its supervision by a capable control system is regulated by law.[12] The control system consists of fixed controls incorporated in the processes and independent control instances, e.g., internal auditing. It is discussed in how far this requirement affects enterprises other than public limited companies.[13] The parent company of a group has to enforce the system across the group, in as much going concern perils may arise from its subsidiaries.[14] The legislator knowingly kept silent on the structure and organisation of the risk early recognition system to allow firm-specific solutions.[15] Various proposals have been

---

7 See *Helten* (1994), p. 21.
8 See *Borch* (1968), pp. 166-180.
9 For a critical view of this limitation see *Baetge/Schulze* (1998), pp. 939-940.
10 See *Deutscher Bundestag* (1998), p. 15.
11 See e.g., *Solomon/Solomon/Norton/Joseph* (2000), pp. 451-453; *Vaughan* (1997), p. 34.
12 See *Gernoth* (2001), pp. 299-300.
13 See *Drygala/Drygala* (2001).
14 See *Deutscher Bundestag* (1998), p. 15; for factual and legal barriers of implementation see *Hommelhoff/Mattheus* (2000).
15 *Deutscher Bundestag* (1998), p. 15.

presented in the literature[16] and by the auditing profession,[17] which all share the above mentioned system components.

Acquisition, analysis, and evaluation of risk by means of risk early recognition may be seen as a prerequisite for the disclosure of the risks of future development of the enterprise or group in the management report or group management report.[18] This risk report is mandatory pursuant to HGB §§ 289, para. 1, clause 2, 315, para. 1, clause 2. The disclosure in the (group) management report shall enhance transparency on the economic status of the firm or group. The risk report is a German specific so far. There are no comparable international standards on risk reporting.[19] However, from 2005 on, the Directive 2003/51/EC requires a company and a group in the European Union to report on "the principal risks and uncertainties that it faces"[20]. This may be seen as a European counterpart of the German legislation existing since 1998. Since neither the law nor the related legislation material specifies the requirements, the statements of private standard setting bodies may be considered for form and contents of risk reports. These are RS HFA 1[21] of the German Institute of Certified Public Accountants (*Institut der Wirtschaftsprüfer, IDW*) and more comprehensive GAS 5 of the *German Accounting Standards Board* (GASB)[22]. GAS 5 applies to risk disclosure in the group management report, but its application is recommended for risk disclosure in the management report, too. Correspondingly, the risk report shall include a description of the risk management process, qualitative and quantitative data on significant risks classified into risk categories, statements of actual or intended measures of risk policy, and their anticipated effects on the corporate risk position. Thus, the risk report shall provide information exceeding the information acquired by the risk early recognition system.[23]

2.2. The Auditor's Role in Supervising Corporate Risk Management

A major target of the Law of Corporate Control and Transparency was the enhancement of corporate governance of German listed companies. While the United States or the United Kingdom rely on one-tier boards, Germany retains its two-tier board system.[24] At least in German public limited companies the supervisory board controls the managing board.[25] The supervisory board is supported by the auditor in fulfilling its monitoring task.[26] To assure his distance to the management board the auditor of a German public listed company is assigned by the supervisory board.

---

16 See e.g., *Emmerich* (1999).

17 See *IDW* AuS 340, para. 3-18.

18 German corporations which are at least medium sized and groups must present a management report besides the annual accounts. It essentially includes a description of the economic situation of the company or group and a description of the development of the business according to HGB §§ 289, 315. The management report is a disclosure particularity in the EU and thus in Germany. It is generally comparable but not on par with the OFR or MD&A in other accounting systems. For the legal demands on the management report see *Ballwieser* (2001), pp. 1331-1332.

19 For the recent discussion in the United Kingdom arising from the Turnbull Report see *Solomon/Solomon/Norton/Joseph* (2000), pp. 453-455.

20 Directive 2003/51/EC, Article 1, No. 14(a); Article 2, No. 2(a)). The Dirctive 2003/51/EC is available at http://europa.eu.int/index_en.htm.

21 See *IDW* RS HFA 1, para. 29-36.

22 The German Accounting Standards Board (GASB) is a private standard setting body developing standards on group accounting. The application of the standards is also recommended in individual accounts. For details see *Ordelheide* (2001), pp. 1365-1368.

23 For empirical findings on risk reporting of German DAX companies see *Kajüter/Winkler* (2003).

24 For corporate governance and the two-tier board structure in Germany see basically *Hopt* (1998).

25 For comments on the practice of the German supervisory board see *Semler* (1998).

26 The Law of Corporate Control and Transparency re-emphasised the auditor's role as the supervisory board's partner, which had been underlying the introduction of statutory annual audits of public limited companies in 1931.

Interpreting AktG § 91, para. 2 as clarification of the managing board's general duties of care and control, two major purposes of the obligation of a risk early recognition system are to be recognised:[27] First, the risk early recognition system of public listed companies must be audited by an independent external authority according to HGB § 317, para. 4. And second, the supervisory board obtains information on the system by means of the auditor's report, assisting the supervisory board's monitoring task.[28]

Besides the supervisory board, the auditor has to check the risk report according to HGB § 317, para. 2. The auditor's conclusions of an investigation are communicated in writing by the auditor's report (HGB § 321) and the audit opinion (HGB § 322).[29] *Figure 1* summarises the various elements of the risk management process and its supervisory institutions.

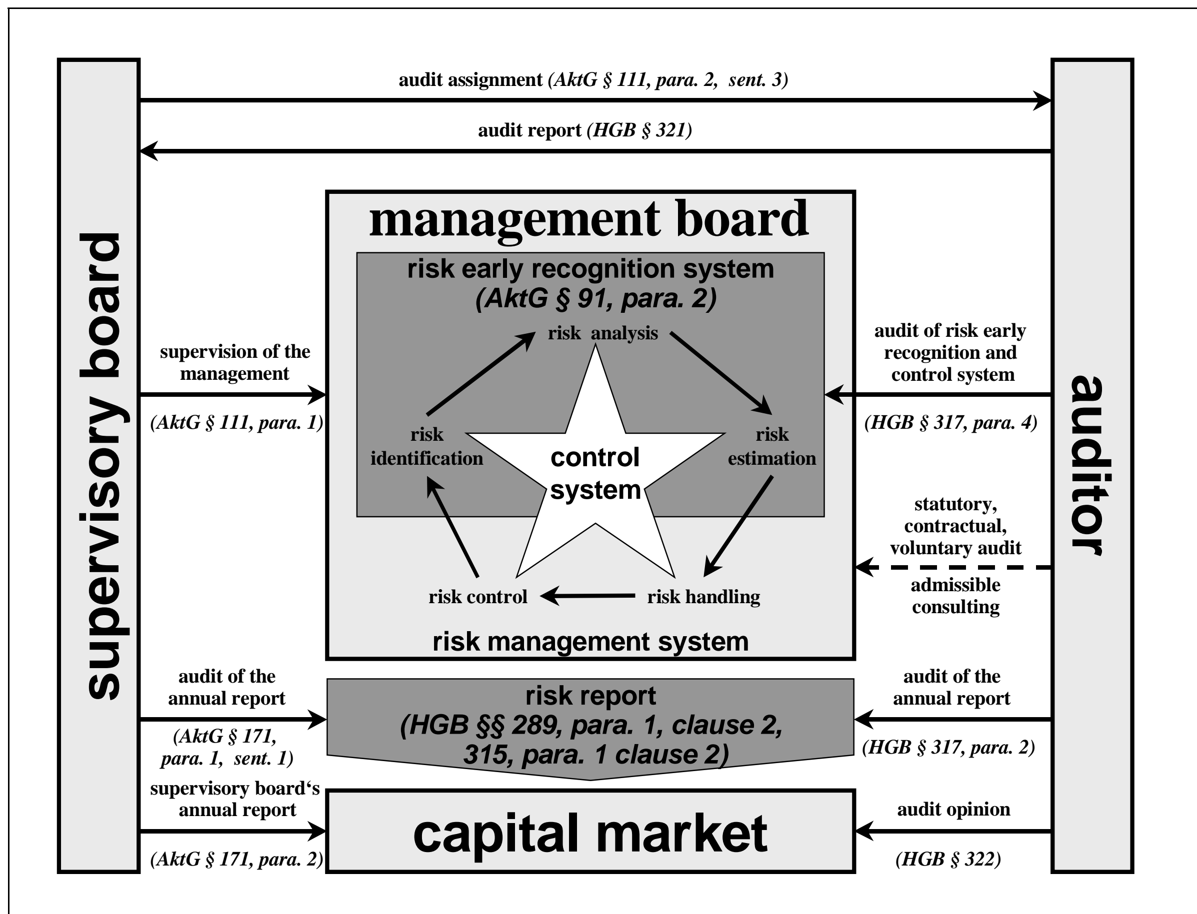

Figure 1: Supervision of Corporate Risk Management

In the context of corporate risk management the auditor's main function is to safeguard the reliability of the corporate risk report and the compliance of the risk early recognition system with legal requirements. The management board's and other decision-makers' responses to risks taken into account and communicated are not in themselves matter of a mandatory audit according to HGB § 317, para. 4.[30] But the auditor may have to consider counter measures to detected risks for assessing the company's ability to continue as a going concern. Moreover, the auditor may influence corporate risk policy within the scope of allowed consulting or of statutory, contractual or voluntary audit mandates.[31] Indeed, the selection, implementation and effect of reaction strategies following detected and communicated risks must be evaluated by

[27] See *Hommelhoff/Mattheus* (1998), p. 251.
[28] For the supervisory board's task to monitor corporate risk management see *Salzberger* (2000).
[29] See *Ballwieser* (2001), pp. 1337-1338.
[30] See *IDW* AuS 340, para. 6.
[31] See *Gelhausen* (1999), p. 395.

the supervisory board. The board may interview the auditor well directed to corporate risk management at the relevant board (or audit committee) meetings.

The law abstractly regulates the audit subjects and the audit criteria. But it fails to supply the auditor either with an exact specification of the risk early recognition system and the risk report or with concrete auditing procedures. The Auditing Standards of the *IDW* may assist the auditor. These standards may be regarded as interpretations of principles of proper auditing by the German auditing profession. Indeed, German auditors are bound to apply these standards in a factual way. But as the standards are no legislation or adjudication, they cannot bind auditors legally. In a specific case the county court of Duisburg decided that the bulletins of the *IDW* may have particular authority, but cannot substitute legal interpretation by courts.[32] *IDW* Auditing Standard 340 deals with "The Audit of the Risk Early Recognition System Pursuant to § 317(4) HGB". It must be seen in the context of legal requirements and other *IDW* Auditing Standards. In practice, the auditing firms individually supplement this particular standard by circular letters.

3. Audit of Corporate Risk Management Components

3.1. Audit of the Risk Early Recognition System

3.1.1. Audit Method and Audit Criteria

The risk early recognition system and its linked internal control structures are subject to the audit according to HGB § 317, para. 4. Main type of audit tests are tests of controls.[33] In general, tests of controls are directed toward the effectiveness of the design and the operating effectiveness of the system and its components.[34] Thus, law and the corresponding legislation material designate the audit criteria existence, eligible design, and operating effectiveness of the measures according to AktG § 91, para. 2.

Audit planning requires a critical analysis of the company's specific risk situation, the risk behaviour of management and of employees.[35] This assessment of inherent risk and control risk is a basis for the application of the concept of audit risk, which meanwhile is used by all major audit firms.[36] Parts of the literature even regard the obligation to audit the risk early detection system as legal basis of the concept of audit risk.[37] In fact, the audit scope was enlarged by the implementation of the statutory audit requirement of the risk early recognition system. It takes into account not only accounting and internal control of accounting procedures, but all business operations from which material risks may arise. When testing the system across the group the auditor will face informational problems if he cannot access the systems of group enterprises and/or use the work of other auditors.[38] Usually, the risk early recognition system is audited as a preaudit or an interim audit. This eases time pressure and enables the auditor to consider gathered perceptions for planning the audit of the financial statements. However, it remains vague whether audit emphasis may vary through the years.

---

[32] See *Amtsgericht Duisburg* (1994).

[33] See *Giese* (1998), p. 453; *IDW* AuS 340, para. 19.

[34] See *Carmichael/Willingham/Schaller* (1996), pp. 107-108; *Arens/Loebbecke* (1997), pp. 313-316.

[35] See *IDW* AuS 340, para. 22.

[36] For an analysis of the concept of audit risk see e.g., *Huston/Peters/Pratt* (1999).

[37] See *Giese* (1998), p. 458; *Pollanz* (2001), p. 1320.

[38] For group specific audit procedures see *IDW* AuS 340, para. 34-37.

3.1.2. Audit Procedures

3.1.2.1. Recognition of System Components

The documentation of the company's risk early recognition system is the auditor's primary information instrument.[39] The documentation has to explain appropriately the organisation and the flow structure of the system with special regard to corporate objectives, reporting and responsibilities in personal, factual and temporal respects.[40]

First, the auditor has to take inventory of the firm's risk early recognition system by means of the documentation in order to ascertain the thorough and corporation-wide existence of provisions according to HGB § 91, para. 2 HGB. A missing, incomplete or deficient documentation may cast doubt on the system's stable operativeness.[41] In lack of a documentation provided by the company, the auditor has to record the system by observation and/or survey.[42] However, some argue that the risk early recognition system could not be audited if a documentation is not provided,[43] while others dread issues of the auditor's independence in the auditor documenting the system.[44]

3.1.2.2. Test of Effectiveness of the System's Design

The effectiveness of the design of relevant measures must be evaluated respecting the legislator's requirements towards the risk early recognition system. This demands a precocious detection of undesirable future developments at a date at which suitable counter measures still may be taken.[45] Therefore, the auditor particularly has to test[46]

(1) the completeness and flexibility of coverage of internal and external risk areas;
(2) the completeness, earlyness, and appropriateness of identification of relevant risks by suitable indicators;
(3) the comprehensibility and plausibility of risk analysis and risk estimation by means of suitable methods;
(4) the verifiability and timeliness of the communication of notifiable risks to settled responsibles; and
(5) the adequateness of internal control in personal, functional, and temporal respect.

The completeness of risk detection, especially pertaining to weak signals, may not be fully assessed due to incomplete foresight. Regarding risk evaluation, the auditor has to test if the system is able to transform the amount of detected signals into material and immaterial risks considering the danger for a going concern. As the probability of risk occurrence, the anticipated extend of damage predominantly result from the management's subjective beliefs of credibility, the auditor merely may evaluate the plausibility of the estimations.[47] Moreover, the auditor encounters problems by evaluating measurements of materiality concerning the internal obligations to report as well as the continuing of the company as a going concern.[48]

---

39 See *IDW* AuS 340, para. 23-24.
40 For a check-list see *IDW* AuS 340, para. 17.
41 See *IDW* AuS 340, para. 24; *Pollanz* (2001), p. 1323.
42 See *Giese* (1998), p. 453; *IDW* AuS 340, para. 25.
43 See e.g., *Förschle/Peter* (1999), para. 89.
44 See e.g., *Pollanz* (2001), p. 1321.
45 See *Deutscher Bundestag* (1998), p. 15.
46 See *Giese* (1998), p. 453-457; *IDW* AuS 340, para. 26-30; basically following this standard *Böcking/Orth* (2000), pp. 251-252.
47 See *Giese* (1998), pp. 455-456.
48 For an analytical approach see *Ro* (1982). In practice, materiality pertains to fixed measures of accounting data.

Investigating the plausibility of information generated by the risk early recognition system may be assisted by substantive analytical tests involving the study and comparison of relationships among the audit subject and related information.[49] This implies the knowledge of suitable objects of comparison acquired by the auditor from actions for the company considered or another company. However, the auditor has to obey regulations on discretion.[50] In the case of specific, i.e. technical risks it may be necessary to consult a surveyor.

3.1.2.3. Test of the System's Operating Effectiveness

Based upon the perceptions on existence and eligible design of the risk early recognition system the auditor has to investigate its operating effectiveness and continuous application throughout the period under audit. The auditor has to test whether the relevant process rules have been observed persistently. Analytical procedures and/or sampling methods may be used. In particular the auditor has to assess

(1) risk identification, analysis, estimation, and communication by means of observation, survey and/or records;[51] and
(2) the control system on the basis of working papers and audit programs of the institutions of internal control.[52]

Hereby, the auditor must consider whether the kind or the date of independent controls may be anticipated impairing the purpose of the controls. As the risk early recognition system and related internal controls are not monitored throughout the entire period being audited, the auditor cannot definitively exclude, that process rules have been suspended temporarily.

3.2. Respectiveness of the Audit of the Risk Report

While auditing the risk early recognition system does not individually require an evaluation of the managing board's reactions on detected and communicated risk information, this may become necessary with respect to the audit of the (group) risk report. The risk report as part of the management report must be examined to determine

(1) whether it agrees with the financial statements;
(2) whether it is in compliance with the auditor's perceptions gathered in the course of the audit;
(3) whether it gives a fair impression of the position of the enterprise or group; and
(4) in particular whether the risks of future development are presented fairly (HGB § 317, para. 2).

It is known that the accuracy of forecasts cannot be verified at an ex ante stage, but the auditor can merely assure that the data published has not been prepared recklessly or in bad faith. This has been discussed copiously when corporate forecasts became a mandatory part of disclosure.[53] Thus, the German legislator charges the auditor with examining whether all forthcoming information was used, whether the assumptions were realistic and consistent and whether forecast techniques were applied properly.[54] The audit of the risk report aims at

---

49 See *Carmichael/Willingham/Schaller* (1996), pp. 155-159.
50 See HGB § 323; and WPO § 43, para. 1.
51 See *Giese* (1998), p. 457.
52 See *IDW* AuS 340, para. 31.
53 See e.g., *Brown* (1972); *Carmichael* (1974); *Corless/Norgaard* (1974).
54 See *Deutscher Bundestag* (1998), p. 27.

integrity, plausibility and clarity. However, German auditors regard this as immense challenge.[55] For what reasons?

Without the need for discussing the relevant audit procedures in detail,[56] the association between the audit of the risk early recognition system and the audit of the risk report becomes evident: On the one hand the auditor must revert to the perceptions of testing the system for evaluating the fair impression of the risk report, on the other hand the risk report should support the auditor's risk assessment. As the risk report has to contain information on risk handling and its presumed effects, to a certain extent, the audit of the risk report refers to risk management as a whole. The respectivness becomes manifest, when the risk report describes corporate risk management, as required by GAS 5, para. 28-29. As far as it is required to evaluate the risk report,[57]

(1) the auditor must regard risk handling and risk control besides the measures according to AktG 91, para. 2;
(2) the whole risk management process becomes relevant for the auditors of companies (other than public listed ones), which have to disclose management reports;
(3) not only detected risks in the narrower sense, but in the broader sense must be considered, which also have to be presented as forecasts in the management report.

3.3. Audit Results

The auditor must report in writing on the results of the investigation.[58] The audit report is addressed to the supervisory committee. The auditor's opinion is published along with the annual report.

Besides stating whether the enterprise is considered to be a going concern and besides fixing whether the risk report and the group risk report comply with legal requirements, a separate part of the audit report has to show the outcome of the audit of the risk early recognition system.[59] Whether procedures to improve the system are considered to be necessary must be mentioned.[60] If there are no objections, reporting may be reduced to this statement.[61] Neither the law nor the standards of the *IDW* require to include a description of the system or concrete suggestions of its improvement.[62]

The audit opinion expresses the final conclusion on management's fulfilment of legal requirements. The audit opinion must consider going concern uncertainties and fair presentation of the risk report among other statements.[63] Objections concerning the risk early recognition system do not affect the audit opinion.[64] But they may become relevant, if pitfalls of the system result in misleading presentation of the risk report or other parts of the financial statements.

---

55 See *Dörner* (1998), p. 304.
56 See *IDW* AuS 350, para. 13-18.
57 See recapitulatory *Dobler* (2001), p. 2090.
58 In Germany, the management letter lacks a legal basis, but it may still be common use.
59 See HGB § 321, para. 4; recently revised *IDW* AuS 450, para. 104-107.
60 See *Ballwieser* (2001), p. 1337.
61 For the recommended formulation see *IDW* AuS 450, para. 105.
62 See *IDW* AuS 450, para. 106.
63 See HGB § 322, para. 2, sent. 2; and para. 3, sent. 2; *IDW* AuS 400, para. 63, 77-79.
64 See *IDW* AuS 340, para. 10; doubting *Böcking/Orth* (2000), pp. 253-255.

4. Discussion

4.1. Expectation Gap and Criteria to Discuss

A major objective of the changes implemented by the Law of Corporate Control and Transparency was the diminution of the expectation gap in auditing.[65] The expectation gap may be defined as „the gap between society's expectations of auditors and auditors' performance, as perceived by society.“[66] The expectation gap may be divided into a performance gap and a reasonableness gap. The performance gap derives from deficient audit performance and/or deficient auditing standards, while the reasonableness gap reflects unreasonable public expectations of auditing.[67] Due to inhomogeneous expectations, needs, interests and preferences and in public the gap may not be generally bridged. But the expectation gap can be reduced by enlarging audit scope and improving audit quality as well as by extending the information presented in both the audit report and the audit opinion. Reflecting to these criteria, major arguments concerning the (possible) impact of the requirement to audit risk management components on the expectation gap shall be discussed.

4.2. Scope of Application

In general, audit scope is enlarged by the mandatory audit of the risk early recognition system. Formerly, the legal requirement of an audit according to HGB § 317, para. 4, solely pertained to public limited companies with officially quoted shares in the segment of the *Amtlicher Handel*. Due to both academic criticism and public preasure driven from further corporate crises, the personal scope of application has been enlarged to all public limited companies. This aims at building public trust.

The risk reports of all listed companies and groups – among others – must be audited. Due to the coherence of the audit of the risk report and the audit of the risk early recognition system, some argue that a test of the system was mandatory for those enterprises disclosing risk reports.[68] But since the audits have different focuses as discussed above, the audit of the risk report cannot substitute the audit of the risk early recognition system according to HGB § 317, para. 4. Those who do not argue likewise must see that the requirement of disclosing the risk report is just a clarification of the duty of disclosing a management report. Moreover, the requirement to audit the risk report merely points out the requirement to audit the management report. If auditing the risk report as integral part of the management report demanded an audit according to HGB § 317, para. 4, this would have been required since the mid-80's, when the management report and its audit became mandatory. This conclusion may go well too far. Thus, the requirement of auditing the risk early recognition system pursuant to HGB § 317, para. 4 in itself does not affect enterprises other than public listed companies.

4.3. Audit Scope

The new legislation has charily strengthened the risk and future orientation of annual audits. The auditor may no longer focus on accounting and related internal control, but he must consider all corporate risk spheres. To a great extent society seems to expect a mandatory management audit as task of annual audits.[69] But auditing the risk early recognition system merely focuses on the fulfilment of the legal requirements of implementing an adequate and

65 See *Deutscher Bundestag* (1998), p. 11.

66 *Porter* (1993), p. 50.

67 See *Liggio* (1973), p. 27; *Porter* (1991).

68 See *Pollanz* (2001), p. 1320.

69 For empirical evidence in Germany see *Ruhnke/Deters* (1997), p. 932.

operative monitoring system to detect material risks.[70] Though this audit comprehends constituents of a management audit, it is none. That is mainly because management's reactions on the risk information communicated are no subject to the audit according to HGB § 317, para. 4 and because efficiency and expediency of these reactions need not be assessed by within the audit of risk reporting.[71] This solely remains the supervisory board's task. Thus, just a further enlargement of audit scope might help to approach public expectations in auditing. However, a recent inquiry among representatives of 96 German insurance companies shows that the management boards award themselves more competence in monitoring corporate risk management than the auditor or the supervisory board.[72]

4.4. Information Provided by the Audit Report

The audit report informs the supervisory committee about the outcome of the auditor's investigations. The actual information content of audit reports and information exchange at the board meeting accompanied by the auditor may hardly be assessed by an external viewer. The enhancement of audit scope along with increased requirements concerning the audit report suggests a more comprehensive information of the supervisory board. But following the auditing profession's view explained in the Audit Standard of the *IDW*, the audit report does not need to contain concrete suggestions of measures for improving the risk early recognition system. Therefore, the advisory committee might barely obtain information of sub-systems or processes which are suggested to be improved.[73] Ostensibly, this information has to be achieved by further consulting mandates.

4.5. Information Provided by the Audit Opinion

While little may be said on the audit report, the audit opinion is publicly available. Following the Auditing Standards, the audit of the risk early recognition system does neither affect attestation nor needs it to be recorded in the audit opinion. Therefore, the user does not obtain information on the outcome of the audit of the risk early recognition system and even whether it was actually audited.

The following empirical investigation highlights these deficits. I studied the audit opinions of 81 German parent companies listed in the DAX using the companies' annual reports of the fiscal year 1999 or 1999/2000.[74] These were the first fiscal years in which the new accounting and auditing legislation was applied mandatorily. My key findings are:

(1) All certificates were drafted unqualified, there were no qualifications or disclaimers of the audit opinion.
(2) Two opinions remark substantial doubt about the entity's ability to continue as a going concern (HGB § 322, para. 2, sent. 2).[75]
(3) No audit opinion indicates the audit of the risk early recognition system.
(4) Six audit opinions fail to record that the risks of the future development are reflected adequately (HGB § 322, para. 3, sent. 2).[76]

---

[70] See *IDW* AuS 340, para. 19.

[71] See *Mattheus* (1999), pp. 703-704, 706-707.

[72] See *Gabriel/Rockel* (2001), p. 128.

[73] See *Moxter* (1997), pp. 726-729; *Dobler* (2001), pp. 2090-2091.

[74] The sample includes the companies listed in the DAX on December, 30th 1999. This date corresponds with the underlying fiscal years. Twelve banks and seven insurers were eliminated due to specific regulations in these sectors.

[75] *Philipp Holzmann AG* and *Spar Handels-AG*.

[76] *Adidas-Salomon AG*, *DaimlerChrysler AG*, *Fresenius Medical Care AG*, *Merck KGaA*, *Südzucker AG* and *Tarkett Sommer AG*.

The latter is noteworthy because it is exclusively related to the audit opinions concerning group accounting according IAS or US-GAAP issued by *KPMG*. These audit opinions explain in one case that US-GAAS and German standards on auditing were applied and in the remaining six cases that solely ISA or US-GAAS were applied. As neither IAS nor US-GAAP require risk reports comparable to German law, it is not amazing that neither ISA nor US-GAAS claim the comment on adequate presentation of the risk report. HGB § 292a allows to substitute group accounts according to the German company law for accounts according to IAS or US-GAAP when fulfilling certain conditions.[77] But this does not relieve the group accounts to be audited according to the German company law. Regardless of the discussion on the admissibleness of audit procedures according to ISA or US-GAAS in Germany, the audit report must include the statement as required by German company law.

Anecdotal evidence shows, that this deficit of audit opinions printed in German annual reports exists to date. However, this finding should not be misinterpreted. The annual reports examined are not directly required by law. Besides the obligatory instruments of financial reporting, the genuine audit opinion has to be published in the commercial register (*Handelsregister*) and the federal gazette (*Bundesanzeiger*).[78] Because I did not check those audit opinions comparatively, it must not be concluded that the auditor's audit opinion did not comply with German legal requirements. However, it seems common corporate practice to publish condensed or alternative audit opinions in the voluntary annual reports. This is dissatisfying. As the annual reports are still the main source of corporate information used by German investors, withholding the genuine audit opinion gives rise to possible misinterpretation, lack of understanding, and investor scepticism. This may undermine public trust in accounting and auditing. If the auditor suffered disadvantages by the company's inadequate presentation of his audit opinion or fears to, he will work towards the publication of the genuine audit opinion in the annual report.

Indeed, the statement that the risks of future development were reflected adequately may result in excessive expectations and thus in an expectation gap.[79] The reason is that the auditor is no clairvoyant. He merely and under the shown restrictions may test the plausibility, but not the truth of management's evaluation of the future developments and the resulting risk position.

Thence, it may be doubted that the introduction of HGB 317, para. 4 has materially contributed to a reduction of the expectation gap in auditing. The discussion of further modifications of audit requirements regarding corporate risk management is indispensable in Germany as well as in an international context.

5. Conclusions

(1) The management boards of German public listed companies are required to set up a risk early recognition system to timely detect risks endangering the company to continue as a going concern. The systems are subject to the annual audit. Hereby, the auditor faces substantial vagueness arising from two sources. First, the legislator fails to specify the audit subject. Second, no audit procedures are appointed by legislation and there are no comparable issues in other countries. The auditor may be assisted by the standards of the German Institute of Certified Public Accountants (*IDW*), particularly by Auditing Standard 340 dealing with the audit of the risk early recognition system. These standards oblige auditors in a factual, but not in a legal way.

---

[77] See *Ordelheide* (2001), pp. 1369-1370, 1380.

[78] See *Ballwieser* (2001), pp. 1338-1340.

[79] See *Moxter* (1997), pp. 722-723.

(2) The auditor has to ascertain the existence, effectiveness of design, and operating effectiveness of the risk early recognising system by means of tests of controls. This includes the investigation of the sub-systems risk identification, risk analysis and risk evaluation as well as communication and control processes. Primal problems arise from the prospective and subjective character of risk assessment. The auditor merely has to evaluate risk handling and its expected impacts if this is necessary to give an opinion on the fulfilment of legal requirements concerning the risk report. While the outcome of the audit of the risk early recognition system is presented in a separate part of the audit report, it does not affect the audit opinion.

(3) The audit of the risk early recognition system expands the audit scope to non-accounting areas and covers components of a management audit. But it solely remains the supervisory board's task to evaluate efficiency and expediency of risk measures and risk management as a whole. This and the deficit reporting requirements and practice may not be suitable to fulfil public expectations of auditing corporate risk management. An empirical investigation on audit opinions of companies listed in the DAX 100 highlights that audit opinions published in the annual reports do not comply with German legal requirements in cases of audits according to ISA or US-GAAS. This may undermine public trust, which was intended to be built by the audit requirements surrounding corporate risk management.

References

Amtsgericht Duisburg (1994): Beschluß vom 31.12.1993, 23 HR B 3193, in: Der Betrieb, 47 (1994), pp. 466-467.

Arens, Alvin A./Loebbecke, James K. (1997): Auditing, an integrated approach, 7th edition, Upper Saddle River 1997.

Baetge, Jörg/Schulze, Dennis (1998): Möglichkeiten der Objektivierung der Lageberichterstattung über „Risiken der künftigen Entwicklung“, in: Der Betrieb, 51 (1998), pp. 937-948.

Ballwieser, Wolfgang (2001): Germany – Individual Accounts, in*: Ordelheide, Dieter/KPMG* (eds.): Transnational Accounting, 2nd edition, New York 2001, pp. 1217-1351.

Böcking, Hans-Joachim/Orth, Christian (2000): Risikomanagement und das Testat des Abschlußprüfers, in: Betriebswirtschaftliche Forschung und Praxis, 52 (2000), pp. 242-260.

Borch, Karl H. (1968): The Economics of Uncertainty, Princeton 1968.

Brown, Gene (1972): Ethical and Other Problems in Publishing Financial Forecasts, in: Financial Analyst Journal, 28 (1972), pp. 38-45.

Carmichael, Douglas R. (1974): Financial forecasts – the potential role of independent CPAs, in: Journal of Accountancy, 138 (1974), September, pp. 84-87.

Carmichael, Douglas R./Willingham John J./Schaller, Carol A. (1996): Auditing Concepts and Methods, 6th edition, New York et al. 1996.

Corless, John C./Norgaard, Corine T. (1974): User reactions to CPA reports on forecasts, in: Journal of Accountancy, 138 (1974), August, pp. 46-54.

Deutscher Bundestag (1998): Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), Bundestagsdrucksache XIII/9712, 28.1.1998.

Dobler, Michael (2001): Die Prüfung des Risikofrüherkennungssystems gemäß § 317 Abs. 4 HGB – Kritische Analyse und empirischer Befund, in: Deutsches Steuerrecht, 39 (2001), S. 2086-2092.

Dörner, Dietrich (1998): Von der Wirtschaftsprüfung zur Unternehmensberatung, in: Die Wirtschaftsprüfung, 51 (1998), pp. 302-318.

Drygala, Tim/Drygala, Anja (2000): Wer braucht ein Frühwarnsystem?, in: Zeitschrift für Wirtschaftsrecht, 21 (2000), pp. 297-305.

Emmerich, Gerhard (1999): Risikomanagement in Industrieunternehmen – gesetzliche Anforderungen und Umsetzung nach dem KonTraG, in: Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung, 51 (1999), pp. 1075-1089.

Förschle, Gerhart/Peter, Manfred (1999): Teilkommentierung zu § 317 HGB, in: *Budde, Wolfgang D./Clemm, Hermann/Ellrott, Helmut/Förschle, Gerhart* (eds.): Beck'scher Bilanz-Kommentar. Handels- und Steuerrecht, 4th edition, München 1999, pp. 1747-1781.

Gabriel, Andreas/Rockel, Werner (2001): Risikomanagement in Schaden-/Unfall-Versicherungsunternehmen, in: Zeitschrift für die gesamte Versicherungswissenschaft, 90 (2001), pp. 101-137.

GASB: German Accounting Standard No. 5 (GAS 5): Risk Reporting, in: *GASB* (ed.): German Accounting Standards, Stuttgart 2000; in supplements.

Gelhausen, Hans F. (1999): Aufsichtsrat und Abschlußprüfer – eine Zweckgemeinschaft, in: Betriebswirtschaftliche Forschung und Praxis, 51 (1999), pp. 390-406.

Gernoth, Jan P. (2001): Die Überwachungspflichten des Aufsichtsrats im Hinblick auf das Risiko-Management und die daraus resultierenden Haftungsfolgen für den Aufsichtsrat, in: Deutsches Steuerrecht, 39 (2001), pp. 299-309.

Giese, Rolf (1998): Die Prüfung des Risikomanagementsystems einer Unternehmung durch den Abschlußprüfer gemäß KonTraG, in: Die Wirtschaftsprüfung, 51 (1998), pp. 451-458.

Helten, Elmar (1994): Ist Risiko ein Konstrukt? Zur Quantifizierung des Risikobegriffes, in: *Hesberg, Dieter/Nell, Martin/Schott, Winfried* (eds.): Risiko – Versicherung – Markt. Festschrift für Walter Karten, Karlsruhe 1994, pp. 19-25.

Hommelhoff, Peter/Mattheus, Daniela (1998): Corporate Governance nach dem KonTraG, in: Die Aktiengesellschaft, 43 (1998), pp. 249-259.

Hommelhoff, Peter/Mattheus, Daniela (2000): Risikomanagement im Konzern – ein Problemaufriß, in: Betriebswirtschaftliche Forschung und Praxis, 52 (2000), pp. 217-230.

Hopt, Klaus J. (1998): The German Two-Tier Board: Experience, Theories, Reforms, in: *Hopt, Klaus, J./Kanada, Hideki/Roe, Mark J./Wymeersch, Eddy/Prigge, Stefan* (eds.): Coparative Corporate Governance, Oxford 1998, pp. 227-258.

Huston, Richard W./Peters, Michael F./Pratt, Jamie H. (1999): The Audit Risk Model, Business Risk and Audit-Planning Decisions, in: The Accounting Review, 74 (1999), pp. 281-298.

IDW: IDW Stellungnahme zur Rechnungslegung: Aufstellung des Lageberichts (IDW HFA RS 1), in: *IDW* (ed.): IDW Prüfungsstandards (IDW PS), IDW Stellungnahmen zur Rechnungslegung (IDW RS), IDW Standards (IDW S) einschließlich der zugehörigen Entwürfe und Hinweise, Düsseldorf 1999, in supplements.

IDW: IDW Auditing Standard: The Audit of the Risk Early Recognition System Pursuant to § 317(4) HGB (IDW AuS 340), Düsseldorf 2000.

IDW: IDW Auditing Standard: Audit of the Management Report (IDW AuS 350), Düsseldorf 2000.

IDW: IDW Auditing Standard: Generally Accepted Standards for the Issuance of Auditor's Reports for the Audits of Financial Statements (IDW AuS 400), Düsseldorf 2000.

IDW: IDW Auditing Standard: Generally Accepted Standards for the Issuance of Long-Form Audit Reports for the Audits of Financial Statements (IDW AuS 450), Düsseldorf 2004.

Kajüter, Peter/Winkler, Carsten (2003): Die Risikoberichterstattung der DAX100-Unternehmen im Zeitvergleich, in: Zeitschrift für kapitalmarktorientierte Rechnungslegung, 3 (2003), pp. 217-228.

Liggio, Carl D. (1973): The Expectation Gap: The Accountant's Legal Waterloo?, in: Journal of Contemporary Business, 3 (1973), No. 3, pp. 27-44.

Mattheus, Daniela (1999): Die gewandelte Rolle des Wirtschaftsprüfers als Partner des Aufsichtsrats nach dem KonTraG, in: Zeitschrift für Unternehmens- und Gesellschaftsrecht, 28 (1999), pp. 682-714.

McConnell, Donald K./Banks, Gorge Y. (2003): How Sarbanes-Oxley Will Change the Audit Process, in: Journal of Accountancy, 196 (2003), No. 3, S. 49-55.

Moxter, Adolf (1997): Die Vorschriften zur Rechnungslegung und Abschlußprüfung im Referentenentwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich, in: Betriebs-Berater, 52 (1997), pp. 722-730.

Ordelheide, Dieter (2001): Germany – Group Accounts, in*: Ordelheide, Dieter/KPMG* (eds.): Transnational Accounting, 2nd edition, New York 2001, pp. 1353-1449.

Pollanz, Manfred (2001): Offene Fragen der Prüfung von Risikomanagementsystemen nach KonTraG, in: Der Betrieb, 54 (2001), pp. 1317-1325.

Porter, Brenda (1991): Narrowing the Audit Expectation-Performance Gap: A Contemporary Appproach, in: Pacific Accounting Review, 3 (1991), pp. 1-36.

Porter, Brenda (1993): An Empirical Study of the Audit Expectation-Performance GAAP, in: ABR, 24 (1993), Winter, pp. 49-68.

Ro, Byung T. [Materiality, 1982]: An Analytical Approach to Accounting Materiality, in: JBFA, 9 (1982), pp. 397-412.

Ruhnke, Klaus/Deters, Eric (1997): Die Erwartungslücke bei der Abschlußprüfung, in: Zeitschrift für Betriebswirtschaft, 67 (1997), pp. 923-945.

Salzberger, Wolfgang (2000): Die Überwachung des Risikomanagements durch den Aufsichtsrat, in: Die Betriebswirtschaft, 60 (2000), pp. 756-773.

Semler, Johannes (1998): The Practice of the German Aufsichtsrat, in: *Hopt, Klaus, J./Kanada, Hideki/Roe, Mark J./Wymeersch, Eddy/Prigge, Stefan* (eds.): Coparative Corporate Governance, Oxford 1998, pp. 267-280.

Solomon, Jill F./Solomon, Aris/Norton, Simon D./Joseph, Nathan L. (2000): A Conceptual Framework for Corporate Risk Disclosure Emerging from the Agenda for Corporate Governance Reform, in: British Accounting Review, 32 (2000), pp. 447-478.

Vaughan, Emmett J. (1997): Risk Management, New York 1997.

Münchner Betriebswirtschaftliche Beiträge

2000-01 **Hans-Peter Burghof/Christian Hofmann:** Executives´ Compensation of European Banks -Disclosure, Sensitivity and their Impact on Bank Performance, Juni 2000.

2000-02 **Gunther Friedl:** Sequential Investment and Time to Build, Juli 2000.

2000-03 **Hans-Ulrich Küpper**: Cash Flow and Asset Based Interest Calculation in Cost Accounting, Juli 2000.

2000-04 **Nikolaus Franke/Christian Lüthje:** Studentische Unternehmensgründungen – dank oder trotz Förderung? – Kovarianzstrukturanalytische Erklärung studentischen Gründungsverhaltens anhand der Persönlichkeitskonstrukte "Risikopräferenz" und "Unabhängigkeitsstreben" sowie der subjektiven Wahrnehmung der Umfeldbedingungen, Juli 2000.

2000-05 **Burkhard Pedell:** Sunk Costs, Commitment and Strategy, August 2000.

2000-06 **Wolf Frowein:** On the Consistency of Mean-Lower Partial Moment Analysis and Expected Utility Maximisation, Oktober 2000.

2000-07 **Dietmar Harhoff/Joachim Henkel:** Profiting from voluntary information spillovers: How users benefit by freely revealing their innovations, Juli 2000.

2000-08 **Knieps Günter/Hans-Ulrich Küpper/Rene Langen:** Abschreibungen bei fallenden Wiederbeschaffungspreisen in stationären und nicht stationären Märkten, Dezember 2000.

2001-01 **Heinrich Martin Arnold:** Can great companies survive technology shocks? – A literature overview, Januar 2001.

2001-02 **Zsolt Berényi:** Accounting for illiquidity and non-normality of returns in the performance assessment, Juli 2001.

2001-03 **Michael Dobler:** Auditing Corporate Risk Management – A Critical Analysis of a German Particularity, Juli 2001, .überarbeitet im November 2003.

Michael Dobler
University of Munich
Chair for Accounting and Auditing
Ludwigstr. 28/RG IV
D-80539 Munich
Tel.: ++49-89-2180-6307
Fax.: ++49-89-2180-6327
E-mail: dobler@bwl.uni-muenchen.de
http://www.rwp.bwl.uni-muenchen.de

http://www.bwl.uni-muenchen.de