Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Wirtschaft

CARF Luzern 2018

Controlling.Accounting.Risiko.Finanzen.

Konferenzband

Konferenz Homepage: www.hslu.ch/carf

Die Pflicht des Verwaltungsrates zum integralen Risikomanagement in KMU

Extended Abstract

Dr. iur. Mirjam Durrer, Rechtsanwältin
Hochschule Luzern, Wirtschaft, Institut für Finanzdienstleistungen Zug IFZ, Grafenauweg 10, Postfach 7344, 6302 Zug, E-Mail: mirjam.durrer@hslu.ch

Abstract
Da seit der Revision des Obligationenrechts im Jahr 2013 nur noch "grössere Unternehmen" im Lagebericht Aufschluss über die Durchführung einer Risikobeurteilung geben müssen, entfällt diese Berichterstattungspflicht für kleine und mittelgrosse Unternehmen (KMU). Entgegen einer weit verbreiteten Auffassung ist in der Schweiz jedoch kein Verwaltungsrat eines KMU von der Pflicht zur Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagement-Systems befreit. Kommt der Verwaltungsrat dieser Pflicht nicht nach, droht ihm gegebenenfalls nicht nur eine aktienrechtliche Verantwortlichkeitsklage, sondern möglicherweise auch eine strafrechtliche Verfolgung.

In der juristischen Dissertation "Die Pflicht des Verwaltungsrates zum integralen Risikomanagement in KMU" (Durrer Mirjam, Die Pflicht des Verwaltungsrates zum integralen Risikomanagement in KMU, Dissertation Luzern 2016, Zürich/St. Gallen 2017; https://www.dike.ch/Mirjam-Durrer) werden die rechtlichen Grundlagen des integralen Risikomanagement-Systems im schweizerischen Obligationenrecht erläutert und es wird auf bestehende Lücken hingewiesen. Sodann werden das "Enterprise Risk Management – Integrated Framework" von COSO, die Norm ISO 31000 und das "Knowledge Framework" der Hochschule für Wirtschaft in Luzern (HSLU) formell analysiert, materiell miteinander verglichen und auf ihre Praxistauglichkeit für schweizerische KMU-Verwaltungsräte hin überprüft. Die Entwicklung eines rechtlich fundierten und praxisorientierten Lösungsansatzes für die Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagement-Systems mitsamt Handlungsempfehlungen zuhanden des Verwaltungsrates beschliessen diese Dissertation.

Die nachfolgenden Ausführungen sollen einen Überblick über die wichtigsten Erkenntnisse aus der Dissertation ermöglichen und – unter Einbezug von neuesten Erfahrungen aus der Praxis – die Herausforderungen für den Verwaltungsrat bei der Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagement-Systems aufzeigen.

1 Die rechtlichen Grundlagen

Bis im Jahr 2008 gab es im schweizerischen Obligationenrecht (OR) keine expliziten Bestimmungen zur Durchführung einer Risikobeurteilung oder einer internen Kontrolle durch den Verwaltungsrat. Erst mit der Inkraftsetzung von Art. 663b Ziff. 12 OR im Jahr 2008 wurde der Verwaltungsrat verpflichtet, im Anhang der Jahresrechnung Angaben über die Durchführung einer Risikobeurteilung zu machen (Boemle, 2008, S. 457). Der konzeptionelle Fokus lag dabei auf denjenigen **Risiken, welche einen wesentlichen Einfluss auf die Jahresrechnung haben** können. Zudem wurde die Revisionsstelle aufgrund von Art. 728a und Art. 728b OR verpflichtet, im Rahmen der ordentlichen Revision zu prüfen, ob ein internes Kontrollsystem (IKS) im Unternehmen existiert.

Mit der Inkraftsetzung des neuen Rechnungslegungsrechts im Jahr 2013 wurde Art. 663b Ziff. 12 OR aufgehoben. Die Pflicht zur Berichterstattung über die Durchführung einer Risikobeurteilung befindet sich seither in Art. 961c Abs. 2 Ziff. 2 OR, wobei der konzeptionelle Fokus auf den **unternehmensweiten Risiken** liegt (Gerhard, 2012, S. 905). Diese Änderung des Obligationenrechts hat dazu geführt, dass nur noch "grössere Unternehmen" im Lagebericht Aufschluss über die Durchführung einer Risikobeurteilung zu geben haben. Als "grösser" gelten dabei Unternehmen, welche zwei der drei Schwellenwerte 20 Millionen Franken Bilanzsumme, 40 Millionen Franken Umsatzerlös und 250 Vollzeitstellen im Jahresdurchschnitt in zwei aufeinander folgenden Geschäftsjahren überschreiten. Da bei diesen "grösseren Unternehmen" zudem durch die Revisionsstelle geprüft wird, ob ein IKS existiert, haben sie eine IKS-Dokumentation zu erstellen (Atteslander & Cheetham, 2007, S. 32).

Aufgrund dieser Änderung des Obligationenrechts sind KMU gesetzlich nicht mehr verpflichtet, über die Durchführung einer Risikobeurteilung zu berichten. Dies bedeutet jedoch nicht, dass KMU-Verwaltungsräte von der Pflicht zur Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagement-Systems dispensiert wären, im Gegenteil:

Von den vorerwähnten **Berichterstattungspflichten** streng zu trennen sind die **Prüfungspflichten** des Verwaltungsrates. Der Verwaltungsrat hat zu prüfen, ob die Risikobeurteilung (bestehend aus der Identifikation, der Analyse und der Bewertung der unternehmensweiten Risiken) tatsächlich durchgeführt wurde und ob das IKS existiert. Erst nach erfolgter Prüfung kann der Verwaltungsrat über die Durchführung der Risikobeurteilung und über die Existenz des internen Kontrollsystems berichten. Und da diese Prüfungspflichten Ausfluss aus der **Oberleitungspflicht des Verwaltungsrates** gemäss Art. 716a Abs. 1 Ziff. 1 OR sind, gelten sie gänzlich unabhängig von der Unternehmensgrösse und sind somit für **alle Verwaltungsräte von schweizerischen KMU relevant**.

Aus rechtlicher Sicht ist dem Gesetz damit aber noch nicht Genüge getan: Der Verwaltungsrat eines schweizerischen KMU trägt auch die **Handlungspflicht**, die identifizierten, analysierten und bewerteten Risiken des Unternehmens aktiv zu "managen". Dies bedeutet, dass der Verwaltungsrat die Risiken durch aktives Handeln mittels geeigneter Massnahmen zu bewältigen hat.

Im Obligationenrecht finden sich indes keinerlei Anhaltspunkte dafür, was der Verwaltungsrat materiell konkret umsetzen muss, damit er seiner gesetzlichen Pflicht zur Ausgestaltung, Implementierung und Überwachung des integralen Risikomanagement-Systems sorgfältig nachkommt. Ergänzend sind deshalb internationale Normen beizuziehen, welche sich sowohl zum Risikomanagement-System wie auch zum IKS als technische Normen weltweit etabliert haben.

2 Der hilfsweise Beizug technischer Normen

Technische Normen (auf Englisch "Standards" genannt) haben das Ziel, technische Gegebenheiten und Verfahren zu vereinheitlichen (Brühwiler/Romeike, 2010, S. 81). Sie werden in der Regel von privatrechtlichen Organisationen (wie beispielsweise der "ISO", der „Internationalen Organisation für Normung“) erlassen (Brühwiler/Romeike, 2010, S. 81). Da technische Normen nicht vom Gesetzgeber erlassen werden, stellen sie **keine Rechtsnormen** dar und sind somit nicht per se rechtsverbindlich.

Grundsätzlich werden technische Normen somit auf freiwilliger Basis angewendet, auch im Bereich des integralen Risikomanagements. Da technische Normen von den Gerichten jedoch oft zur **Auslegung unbestimmter Rechtsbegriffe** herangezogen werden, können sie durchaus rechtliche Wirkungen entfalten und insbesondere beim Nachweis der Einhaltung des geforderten Sorgfaltsmassstabes helfen. Die Einhaltung einer internationalen Norm kann den Verwaltungsrat im Schadensfall somit darin unterstützen, den Sorgfaltsbeweis zu erbringen. Dies ist insbesondere deshalb wichtig, weil bereits einfache Fahrlässigkeit das Verschulden des Verwaltungsrates begründen kann.

Im Bereich des Risikomanagements haben sich auf internationaler Ebene das "Enterprise Risk Management – Integrated Framework" von COSO (heute: "Enterprise Risk Management - Integrating with Strategy and Performance") sowie ISO 31000 als technische Normen etabliert. Auf nationaler Ebene wurde sodann das "Knowledge Framework" der HSLU entwickelt, welches sich explizit an KMU richtet. Diese drei Frameworks wurden in der vorliegenden Dissertation umfassend analysiert, miteinander verglichen und auf ihre Tauglichkeit für KMU-Verwaltungsräte hin überprüft. Die vertiefte Analyse resultierte darin, dass sich die drei Rahmenwerke für schweizerische KMU aus unterschiedlichen Gründen nur beschränkt eignen. Dies insbesondere deshalb, weil sie sehr komplex und somit nicht auf KMU zugeschnitten sind. Aus diesem Grund drängte sich die Neukonzeption des integralen Risikomanagement-Systems als rechtlich fundierten und praxisorientierten Lösungsansatz geradezu auf.

3 Die Neukonzeption des integralen Risikomanagements als System für KMU

Gemäss der in der Dissertation entwickelten Neukonzeption des integralen Risikomanagement-Systems hat der Verwaltungsrat die Pflicht zur Ausgestaltung, Implementierung und Überwachung des Risikomanagements wie auch der internen Kontrolle – und zwar beides verstanden als **ein einziges, integrales System**. Darin enthalten sind zudem die materiellen Gehalte des **Crisis Management** (CM) und des **Business Continuity Management** (BCM). Diese Neukonzeption führt dazu, dass der Verwaltungsrat lediglich **ein einziges System** aufzubauen und zu pflegen hat, wodurch Schnittstellen und Doppelspurigkeiten eliminiert werden können.

Die nachfolgenden Ausführungen geben einen Überblick über die Neukonzeption des so verstandenen integralen Risikomanagements als System für KMU:

3.1 Die Pflicht zur Ausgestaltung des integralen Risikomanagement-Systems

Das **integrale Risikomanagement-System** ist **Teil des Management-Systems** des Unternehmens. Die Pflicht des Verwaltungsrates zur Ausgestaltung des integralen Risikomanagement-Systems setzt deshalb seitens des Verwaltungsrates ein tiefgehendes Verständnis des Unternehmens voraus. Dies bedingt, dass der Verwaltungsrat den **normativen Rahmen** des Unternehmens (bestehend aus den Werten, der Vision, der Mission und den Zielen) festsetzt (Müller-Stewens/Brauer, 2009, S. 150). Basierend auf dem normativen Rahmen ist sodann die unternehmensweite **Risikopolitik** zu erarbeiten, welche in Einklang mit der Unternehmenspolitik stehen muss. Zudem ist die **Risikokultur** zu stärken, indem das Risikobewusstsein bei sämtlichen Mitarbeitenden gefördert wird.

3.2 Die Pflicht zur Implementierung des integralen Risikomanagement-Systems

Die Pflicht des Verwaltungsrates zur Implementierung des integralen Risikomanagement-Systems stellt die eigentliche Schnittstelle des Risikomanagement-Systems zum **Risikomanagement-Prozess** dar. Der Risikomanagement-Prozess besteht dabei aus der **Risikobeurteilung** (Identifikation, Analyse und Bewertung der Risiken) sowie der **Risikobewältigung**.

3.2.1 Die Risikobeurteilung

Im Prozess-Schritt **Risikobeurteilung** sind die unternehmensweiten Risiken zu identifizieren, zu analysieren und zu bewerten. Dafür gilt es die Schlüsselfrage im Risikomanagement zu beantworten, welche lautet: "Was kann passieren?" (Gruber & Durrer, 2018, S. 13). Für die anschliessende Risikoanalyse sind die bereits identifizierten Gefahren nach (interner oder externer) Ursache und (interner oder externer) Wirkung zu beschreiben. Wichtig ist, dass der Verwaltungsrat als Ausfluss seiner Fürsorgepflicht als Arbeitgeber auch die Anzahl potenzieller Toter und Verletzter angibt, welche ein allfälliger Risikoeintritt nach sich ziehen kann (Gruber & Durrer, 2018, S. 13).

Die anschliessende Risikobewertung erfolgt nach traditioneller Auffassung gemäss der Eintrittshäufigkeit/Eintrittswahrscheinlichkeit und dem finanziellen Schadensausmass. Neuere Tendenzen ziehen jedoch den **Reputationsschaden** in die Risikobewertung mit ein (Gruber & Durrer, 2018, S. 13).

3.2.2 Die Risikobewältigung

Im Prozess-Schritt **Risikobewältigung** erfolgt das eigentliche "managen" der Risiken, wodurch der Verwaltungsrat seiner gesetzlichen Handlungspflicht nachkommt. Zur Risikobewältigung gehört sowohl die Ausarbeitung von **präventiven** wie auch von **reaktiven** Risikobewältigungsmassnahmen (vgl. auch ONR 49000 ff.). Dies bedeutet, dass für jedes Risiko **Sofortmassnahmen** sowie **Notfall-, Krisen- und Kontinuitätspläne** auszuarbeiten sind (Gruber & Durrer, 2018, S. 14 f.). Aufgrund der Fürsorgepflicht des Arbeitgebers sind Risiken, welche einen Verlust an Humankapital nach sich ziehen, bei der Bewältigung **prioritär** anzugehen. Zudem sind die Risikobewältigungsmassnahmen mit den Mitarbeitenden regelmässig einzuüben.

Das "managen" von Risiken hat indes nicht alleine durch den Verwaltungsrat zu erfolgen, sondern kann teilweise delegiert werden. Diese Aufgabenteilung wird insbesondere im "Three Lines of Defense"-Modell ersichtlich (siehe Abb. 1). Dieses zeigt drei voneinander unabhängige „Säulen“ unterhalb des Verwaltungsrates und der Geschäftsleitung auf, welche der Risikosteuerung dienen. Bei einer allfälligen Delegation ist zentral, dass klare Berichterstattungswege definiert werden (Gruber & Durrer, 2018, S. 12). Der Einbezug der externen Revision als vierte Verteidigungslinie ist zudem erwünscht, wird in der Praxis jedoch häufig nicht so umgesetzt (Gruber & Durrer, 2018, S.12).

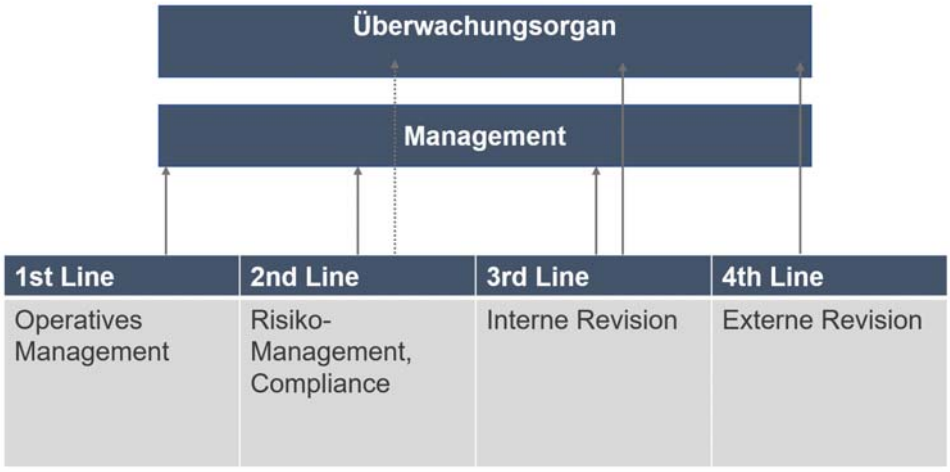

Abbildung 1: Das "Three Lines of Defense"-Modell mitsamt Berichterstattungswegen. Visualisiert durch Dr. Marco Gruber und die Verfasserin.

3.3 Die Pflicht zur Überwachung des integralen Risikomanagement-Systems

Es gehört zu den nicht delegierbaren Aufgaben des Verwaltungsrates, das integrale Risikomanagement-System kontinuierlich zu überwachen und zu aktualisieren. Sowohl die Überwachung wie auch die Aktualisierung haben immer auf sogenannter "best available information" zu basieren (Gruber & Durrer, 2018, S. 14). Aus welchen Quellen diese Informationen stammen ist dabei sekundär – viel wichtig ist, dass die so gesammelten Informationen systematisch ausgewertet und auf ihre Relevanz hin überprüft werden (siehe Abb. 2 als Beispiel für „best available information" in Spitälern). Dies ist insbesondere auch deshalb essenziell, weil dem Verwaltungsrat in einem allfälligen Haftlichtprozess das Wissen zugerechnet wird, welches er hätte haben können. Es ist deshalb dringend zu empfehlen, das integrale Risikomanagement als ständiges Traktandum in den Verwaltungsratssitzungen aufzuführen und das Risikomanagement zudem beweiskräftig zu dokumentieren (Gruber/Durrer, 2018, S. 12 ff.).

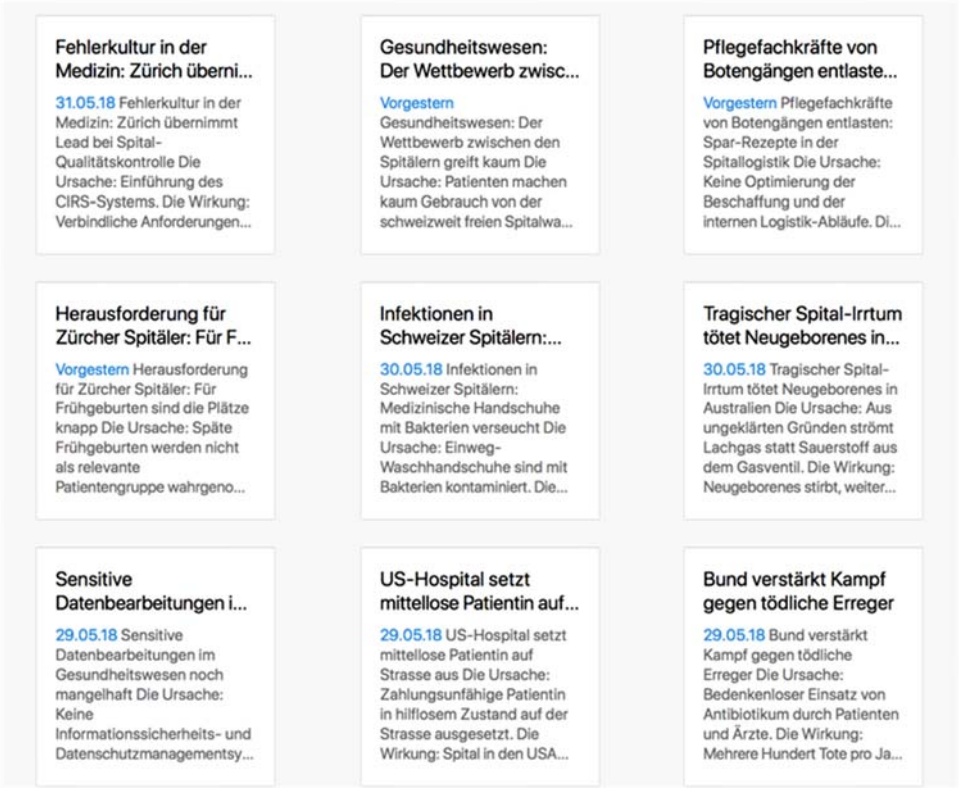

Abbildung 2: "Best available information" am Beispiel von Spitälern im RISKMONITOR®.

4 Ausblick

Abschliessend ist festzuhalten, dass der Verwaltungsrat die Pflicht zur Ausgestaltung, Implementierung und Überwachung des integralen Risikomanagement-Systems ernst zu nehmen hat, auch zur Reduktion des eigenen Risikoprofils. Die Umsetzung internationaler technischer Normen in Kombination mit "best available information" ist deshalb dringend zu empfehlen, da der Verwaltungsrat nur so den heutigen Anforderungen an den Sorgfaltsmassstab genügen kann.

Und da sich im täglichen Leben Einzelrisiken lediglich selten singulär verwirklichen, wird sich der Verwaltungsrat bereits in naher Zukunft auch mit der Verknüpfung von einzelnen Risiken zu ganzen Szenarien befassen müssen (Gruber & Durrer, 2018, S. 13 f.; siehe Abb. 3 als beispielhaftes Szenario „Terroranschlag"). Vor diesem Hintergrund ist davon auszugehen, dass sich diese qualitative Weiterentwicklung des Risikomanagements in einem nochmals erhöhten Sorgfaltsmassstab bei der Beurteilung von allfälligen Pflichtverletzungen durch den Verwaltungsrat manifestieren wird.

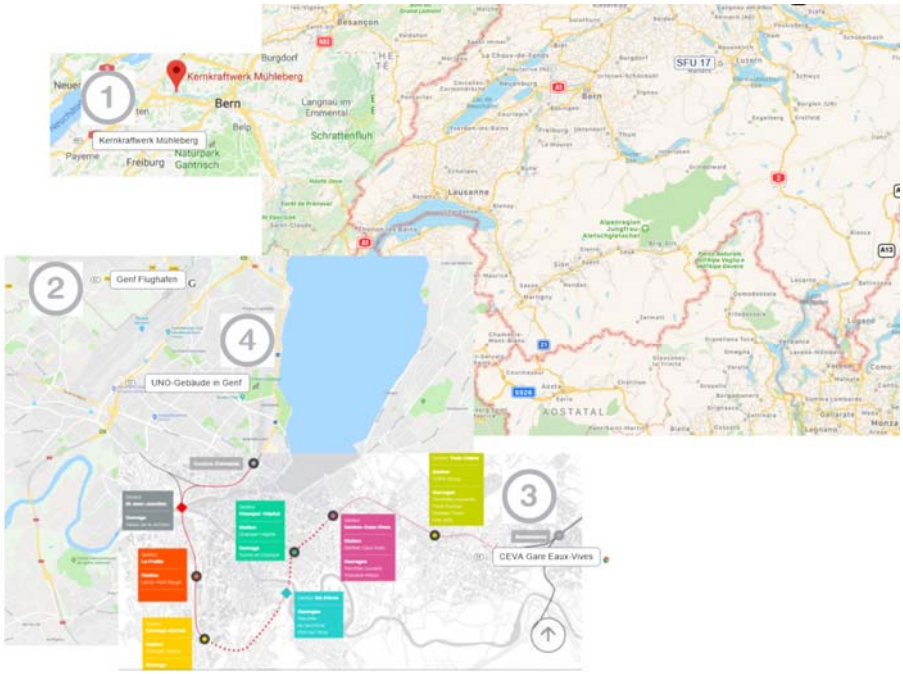

Abbildung 3: Von Einzelrisiken zu Szenarien: Ausschitt aus einer strategischen Führungsübung des Bundes zum Thema Terroranschlag. Visualisierung durch Dr. Marco Gruber und die Verfasserin.

Literaturverzeichnis

Hinweis: Für die Sekundärliteratur wird zudem umfassend auf das Literaturverzeichnis in der Dissertation "Die Pflicht des Verwaltungsrates zum integralen Risikomanagement in KMU" verwiesen.

Atteslander, J., Cheetham, M. (2007): Vorschläge der Unternehmen zum IKS, Definition der Gesetzgebung und die Rolle der Revisionsstelle. ST, 81/2007, S. 30 ff.

Boemle, M. (2008): Opting-out als Regel für Kleingesellschaften. ST, 82/2008, S. 457.

Brühwiler, B., Romeike F. (2010): Praxisleitfaden Risikomanagement, ISO 31000 und ONR 49000 sicher anwenden. Berlin.

Durrer, M. (2017): Die Pflicht des Verwaltungsrates zum integralen Risikomanagement in KMU. Dike, Zürich/St. Gallen.

Gerhard, F. (2012): Der Lagebericht, Allgemeines und Risikobeurteilung (1. Teil). ST, 86/2012, S. 901 ff.

Gruber, M., Durrer, M. (2018): Internationale best practice im integralen Risikomanagement von Spitälern. mt medizintechnik, Ausgabe 4: S. 10-15.

Müller-Stewens G., Brauer, M. (2009): Corporate Strategy & Governance, Wege zur nachhaltigen Wertsteigerung im diversifizierten Unternehmen. Stuttgart.