MIRJAM DURRER
MARCO GRUBER

DER VERWALTUNGSRAT ALS ERSTE VERTEIDIGUNGSLINIE IM INTEGRALEN RISIKOMANAGEMENT

Zur Weiterentwicklung des Three-Lines-of-Defense-Modells im Licht von Art. 716 ff. OR

Der Verwaltungsrat hat die unübertragbare und unentziehbare Rechtspflicht zur Ausgestaltung, Implementierung und Überwachung eines integralen Risikomanagements. Deshalb ist er im schweizerischen Recht als die erste Verteidigungslinie zu bezeichnen. Dies hat Rechtsfolgen mit mehr als bloss numerischen Konsequenzen.

1. RELEVANZ DES THEMAS

Das anerkannte Three-Lines-of-Defense-Modell wird gerne beigezogen, wenn die Verteidigungsorganisation eines Unternehmens gegen Risiken jeder Art bildlich beschrieben werden soll. Dieses Modell geht auf die 8. EU-Richtlinie [1] zurück und hat über die Zeit diverse Präzisierungen erfahren [2].

In organisatorischer Hinsicht sieht das Three-Lines-of-Defense-Modell die folgenden drei Verteidigungslinien als parallel nebeneinanderstehende Silos vor (vgl. *Abbildung*):
→ 1st Line of Defense: operatives Management; → 2nd Line of Defense: Risiko- und Compliance-Management; → 3rd Line of Defense: interne Revision.

Für das Verständnis dieses Modells ist dabei wesentlich, dass der Verwaltungsrat (Board) und die Geschäftsleitung (Senior Management) darin *nicht* als eigentliche Verteidigungslinien, sondern in ihrer Funktion lediglich als Anspruchsgruppen (Stakeholder) geführt sind, welche von den drei echten Verteidigungslinien mit Informationen versorgt werden.

Vorliegend interessiert zunächst, wie sich das Three-Lines-of-Defense-Modell mit dem monistischen Grundkonzept des schweizerischen Aktienrechts gemäss Art. 716 Abs. 2 OR verträgt, wonach sowohl die Überwachungsfunktion als auch die Geschäftsführungsfunktion durch den Verwaltungsrat ausgeübt wird. Denn nach geltendem schweizerischem Recht führt der Verwaltungsrat die Geschäfte der Gesellschaft selbst, soweit er die Geschäftsführung nicht delegiert hat [4].

Zu beantworten ist sodann die Frage, ob der Verwaltungsrat überhaupt – und gegebenenfalls welche – Aufgaben des integralen Risikomanagements rechtmässig an die Geschäftsleitung (und allenfalls weitere Verteidigungslinien) delegieren kann. Denn es ist bereits optisch erkennbar, dass das Three-Lines-of-Defense-Modell grundsätzlich nur bei einer delegierten Geschäftsführung sinnstiftend wirkt und es damit auf mittlere bis grosse Unternehmen fokussiert [5].

2. DIE PFLICHT DES VERWALTUNGSRATS ZUM INTEGRALEN RISIKOMANAGEMENT IM MONISTISCHEN SYSTEM (KEINE DELEGATION DER GESCHÄFTSFÜHRUNG)

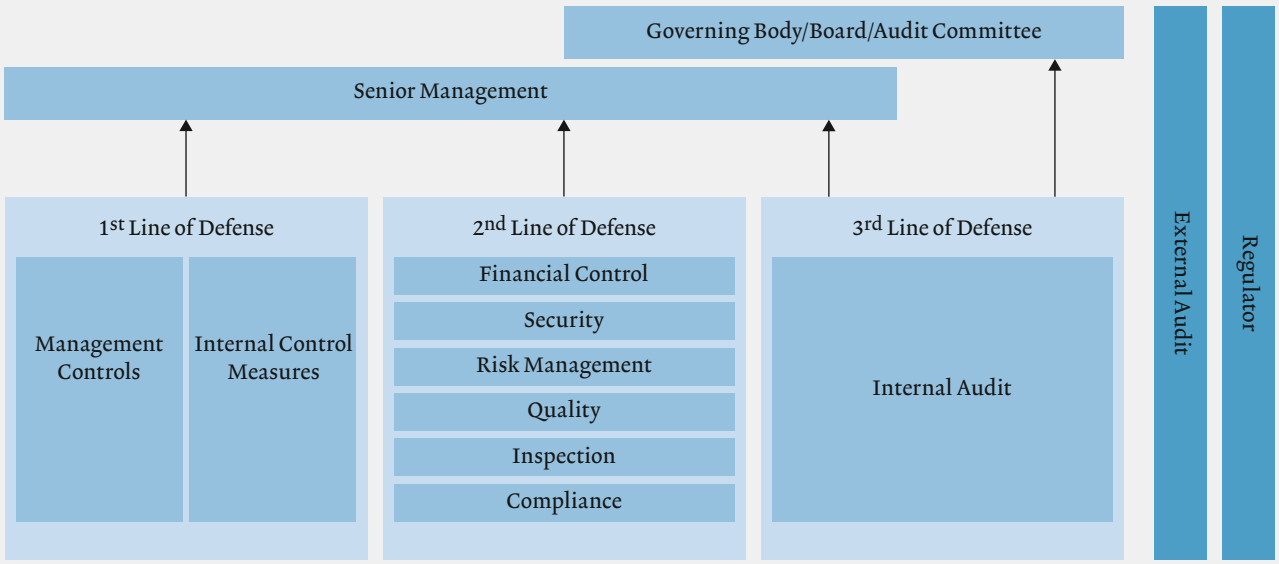
Gemäss Art. 716a OR hat der Verwaltungsrat einen Katalog an Aufgaben, die er weder an die Generalversammlung noch an die Geschäftsleitung übertragen kann. Diese Aufgaben sind somit *unübertragbar und unentziehbar.* Die Oberleitung der Gesellschaft gemäss Ziff. 1 von Art. 716a Abs. 1 OR stellt dabei die Hauptaufgabe des Verwaltungsrats dar. Die übrigen Ziffern dieses Artikels dienen lediglich der Präzisierung dieser Pflicht.

Nebst dem Festlegen, Durchsetzen und Überprüfen der Strategie besteht der Sinn und Zweck der Oberleitungspflicht insbesondere darin, die Gesellschaft vor Risiken zu schützen und dadurch die langfristige Existenz des Unter-

MIRJAM DURRER, DR. IUR., RECHTSANWÄLTIN, DOZENTIN FÜR NORMATIVES BOARD MANAGEMENT, INSTITUT FÜR FINANZDIENSTLEISTUNGEN ZUG IFZ, HOCHSCHULE LUZERN – WIRTSCHAFT

MARCO GRUBER, DR. IUR., FÜRSPRECHER, PARTNER, PROFESSIONELLER VERWALTUNGSRAT, GRUBER PARTNER

Abbildung: **GRAFISCHE DARSTELLUNG DES THREE-LINES-OF-DEFENSE-MODELLS** [3]



Quelle: ECIIA/FERMA, Guidance on the 8th EU Company Law Directive, article 41 (überarbeitete Fassung)

nehmens zu sichern. Dies bedeutet, dass *jeder Verwaltungsrat* gesetzlich dazu verpflichtet ist, ein integrales Risikomanagement auszugestalten, es zu implementieren und zu überwachen [6]. Diese Rechtspflicht gilt unabhängig von der Grösse eines Unternehmens und auch unabhängig davon, ob der Verwaltungsrat in einem Lagebericht Aufschluss über die Durchführung einer Risikobeurteilung zu geben hat. Kommt der Verwaltungsrat dieser Rechtspflicht nicht nach, droht ihm unter Umständen nicht nur eine aktienrechtliche Verantwortlichkeitsklage, sondern eventuell auch eine strafrechtliche Verfolgung.

Das integrale Risikomanagement präsentiert sich dem Verwaltungsrat als ein vielgestaltiger Begriff, dessen Konturen sowohl das Risikomanagement als *System* wie auch als *Prozess* umfassen. Als System integriert das integrale Risikomanagement die Komponenten des internen Kontrollsystems, des Notfall- und Krisenmanagements sowie des Business-Continuity-Managements. Der Prozess des integralen Risikomanagements hingegen besteht aus den beiden Teilschritten der Risikobeurteilung (mit der Risikoidentifikation, der Risikoanalyse und der Risikobewertung) sowie der Risikobewältigung. Letztere sowohl präventiv als auch reaktiv.

Da der Verwaltungsrat im monistischen System die Geschäfte der Gesellschaft selbst führt, ist er selbstredend für sämtliche Aufgaben im integralen Risikomanagement (verstanden als System und als Prozess) zuständig und hat diese eigenhändig wahrzunehmen.

3. DIE PFLICHT DES VERWALTUNGSRATS ZUM INTEGRALEN RISIKOMANAGEMENT IM NICHT MONISTISCHEN SYSTEM (MIT DELEGATION DER GESCHÄFTSFÜHRUNG)

Wie ausgeführt, ist die Rechtspflicht des Verwaltungsrats zum integralen Risikomanagement grundsätzlich unübertragbar und unentziehbar [7]. Es stellt sich daher die Frage, ob der Verwaltungsrat diesbezüglich überhaupt bestimmte Aufgaben an eine Geschäftsleitung delegieren kann.

Dies ist zu bejahen. Es ist zwar unbestritten, dass der Verwaltungsrat aufgrund seiner unübertragbaren und unentziehbaren Pflicht zur Oberleitung der Gesellschaft in der *alleinigen Verantwortung* für seine Führungsentscheide steht. Verfügt das Unternehmen jedoch über eine Geschäftsleitung, kann der Verwaltungsrat ihr im Allgemeinen die Vorbereitung, die Ausführung und die Überwachung seiner Führungsentscheide im Sinn von Art. 716a Abs. 2 OR kraft der Delegationsnorm von Art. 716b Abs. 1 OR zuweisen. Die Aufgabe der Geschäftsleitung besteht diesfalls darin, verschiedene Lösungsvorschläge sowie Handlungsalternativen auszuarbeiten, die dem Verwaltungsrat als Entscheidungsgrundlage dienen [8]. Dies gilt nach der hier vertretenen Auffassung im Besonderen auch für das integrale Risikomanagement und führt dazu, dass der Verwaltungsrat nicht mehr sämtliche damit verbundenen Aufgaben höchstpersönlich ausführen muss. In den nächsten Abschnitten werden im Sinn einer beispielhaften Aufzählung die Aufgaben und ihre Zuweisung aufgeführt.

3.1 Ausgestaltung des integralen Risikomanagements

3.1.1 Nicht delegierbare Aufgaben des Verwaltungsrats. Der Verwaltungsrat muss den Systementscheid fällen, will heissen: Er allein entscheidet zugunsten eines bestimmten integralen Risikomanagementsystems (wie beispielsweise ISO 31000/ ONR 49000 oder COSO ERM) [9]. Orientiert sich der Verwaltungsrat dabei an einer dieser international anerkannten Normen, hat er zu beachten, dass sowohl ISO 31000 als auch COSO ERM im Bereich des Notfall- und Krisenmanagements wie des Business-Continuity-Managements lückenhaft ausgestaltet sind und somit den qualitativen Anforderungen an ein integrales Risikomanagementsystem per se nicht genügen [10].

Zur Ausgestaltungspflicht des Verwaltungsrats gehört es zudem, den normativen Rahmen des Unternehmens zu definieren, der auf den Unternehmenswerten beruht. Diese Unternehmenswerte wiederum dienen dem Konkretisieren von Vision und Mission des Unternehmens. Erst in einem nachgelagerten Schritt können daraus die Unternehmensziele abgeleitet werden. Damit erweitert der Beizug des normativen Rahmens gleichzeitig auch den Risikobegriff, der bislang auf die Auswirkung von Unsicherheit auf Ziele fokussierte. Dies hat zur Folge, dass ein Risiko auch dann vorliegen kann, wenn die Vision oder die Mission eines Unternehmens tangiert ist, nicht mehr zwingend jedoch ein definiertes Ziel [11].

Ist der normative Rahmen als relevante Bezugsgrösse im Risikomanagement bestimmt, hat der Verwaltungsrat die Risikopolitik [12] und die Risikokultur [13] festzulegen. Diese sind aus der Unternehmenspolitik und der Unternehmenskultur des Unternehmens abgeleitet und sollen damit in Einklang stehen.

3.1.2 Vom Verwaltungsrat an die Geschäftsleitung delegierbare Aufgaben. Der Verwaltungsrat kann indes die Vorbereitung sowie die Ausführung des Systementscheids an die Geschäftsleitung delegieren. Dies bedeutet, dass die Geschäftsleitung beispielsweise eine Analyse der infrage kommenden Risikomanagementsysteme vornimmt und diese dem Verwaltungsrat im Sinn von Lösungsvorschlägen präsentiert. Hat der Verwaltungsrat den Systementscheid gefällt, kann die Geschäftsleitung die weitere Ausführung dieses Entscheids übernehmen. Dazu gehört beispielsweise die Evaluation einer geeigneten Risikomanagement-Software.

Auch die Ausformulierung des normativen Rahmens, der Risikopolitik sowie der Risikokultur als Entwurf kann die Geschäftsleitung übernehmen und dem Verwaltungsrat hierzu entsprechende Vorschläge unterbreiten.

3.2 Implementierung des integralen Risikomanagements. Hat der Verwaltungsrat mit der Ausgestaltung des integralen Risikomanagements die formellen Grundlagen einmal gelegt, so geht es nunmehr um die konkrete Implementierung des gewählten Systems ins Unternehmen. Dieser Schritt stellt gleichzeitig die Schnittstelle zum Risikomanagement als Prozess dar.

3.2.1 Nicht delegierbare Aufgaben des Verwaltungsrats. Der Verwaltungsrat hat selbst die Kriterien für die Risikobewertung festzulegen. Dabei beachtet er die unternehmensspezifischen Gegebenheiten, damit er die drei Dimensionen Eintrittshäufigkeit, Schadenshöhe sowie Reputationsschaden definieren kann.

Sodann hat der Verwaltungsrat die Leitplanken für die Priorisierung der Risikobewältigungsmassnahmen zu erlassen und damit die Frage zu beantworten, in welcher Reihenfolge die Risiken planerisch zu bewältigen sind. Dabei sind Risiken mit möglichen Toten und/oder Verletzten aufgrund der Fürsorgepflicht des Arbeitgebers *immer prioritär* zu behandeln.

3.2.2 Vom Verwaltungsrat an die Geschäftsleitung delegierbare Aufgaben. Auch in Bezug auf die Implementierung des integralen Risikomanagements kann der Verwaltungsrat das konkrete Vorbereiten, Ausführen und Überwachen seiner Verwaltungsratsbeschlüsse delegieren. Dazu gehört namentlich:
→ Die Geschäftsleitung identifiziert, analysiert und bewertet die Risiken gemäss den Vorgaben des Verwaltungsrats und unterbreitet diese Risikobeurteilung dem Verwaltungsrat im Sinn eines Vorschlags zur Genehmigung. → Die Geschäftsleitung erarbeitet vorschlagsweise die Risikobewältigungsmassnahmen (inkl. Notfall-, Krisen- und Kontinuitätsplänen) mitsamt Projektplan für die Umsetzung dieser Massnahmen. Dabei orientiert sie sich an den verwaltungsrätlichen Vorgaben zur Priorisierung der Risiken.

3.3 Überwachung des integralen Risikomanagements. Auf die erfolgreiche Implementierung folgt die kontinuierliche Überwachung des integralen Risikomanagements, wozu auch dessen regelmässige Aktualisierung gehört, basierend auf «best available information» [14].

3.3.1 Nicht delegierbare Aufgaben des Verwaltungsrats. Der Verwaltungsrat hat für die adäquate Überwachung des integralen Risikomanagements zu sorgen. Aufgrund seiner Oberaufsichtspflicht gemäss Art. 716a Abs. 1 Ziff. 5 OR kann er diese Pflicht jedoch *nie umfassend* an die Geschäftsleitung delegieren. Dies gilt umso mehr, als der Verwaltungsrat bei Bedarf eine Eingriffspflicht hat.

Damit der Verwaltungsrat seiner Eingriffspflicht nachkommen kann, hat er in Bezug auf die Überwachung des integralen Risikomanagements die folgenden nicht delegierbaren Aufgaben:
a) Um die Vorschläge der Geschäftsleitung in Bezug auf die Risikoidentifikation kontrollieren zu können, muss jeder Verwaltungsrat selbst über «best available information» verfügen. Der Verwaltungsrat hat sich deshalb regelmässig darüber zu informieren, welche internen und externen Ereignisse sich zu potenziellen Risiken für das Unternehmen auswachsen können.
b) Zudem hat der Verwaltungsrat die Veränderungen in der Risikobewertung zu prüfen und zu hinterfragen.
c) Ferner ist zwingend, dass der Verwaltungsrat selbst regelmässig den Stand der Umsetzung aller Risikobewältigungsmassnahmen kontrolliert. Der Verwaltungsrat hat also in seinen Sitzungen periodisch zu überprüfen, ob die festgelegten Bewältigungsmassnahmen auch tatsächlich umgesetzt werden. Gleiches gilt für das Notfall- und Krisenmanagement sowie für das Business-Continuity-Management, deren praktische Einübung er mit Blick auf seinen hohen Sorgfaltsmassstab anzuordnen (und ebenfalls zu kontrollieren) hat.

3.3.2 Vom Verwaltungsrat an die Geschäftsleitung delegierbare Aufgaben. Die Geschäftsleitung kann den Verwaltungsrat bei dessen Pflicht zur Überwachung des integralen Risikomanagements wie folgt unterstützen:
a) Die Geschäftsleitung bereitet die entscheidungsrelevanten Informationen übersichtlich auf, damit der Verwaltungsrat auf einen Blick die Veränderungen im Risikoprofil des Unternehmens erkennt. Dazu gehört, dass die Geschäftslei-

tung dem Verwaltungsrat regelmässig die neu identifizierten und nach Ursache und Wirkung analysierten Risiken unterbreitet, welche bereits im Sinn eines Vorschlags bewertet worden sind.
b) Die Geschäftsleitung kontrolliert und überwacht das Projektmanagement zur Risikobewältigung straff, damit sie dem Verwaltungsrat auf übersichtliche Weise den Stand der jeweiligen Projektumsetzung unterbreiten kann.

4. EINBEZUG DER WEITEREN VERTEIDIGUNGSLINIEN DURCH DEN VERWALTUNGSRAT

Hat der Verwaltungsrat rechtsgültig an die Geschäftsleitung delegiert, kann die Geschäftsleitung selbstverständlich weitere Personen für die Aufgabenerfüllung im integralen Risikomanagement beiziehen. Dazu gehören insbesondere die Risk Owner, also die Risikoeigner, welche für ein ihnen zugewiesenes Risiko in der Verantwortung stehen.

Diese Risikoeigner wiederum bilden zusammen mit der Geschäftsleitung das sog. *operative Management* gemäss dem etablierten-Three-Lines-of-Defense-Modell. Und exakt an dieser Schnittstelle ändert die Nummerierung der Verteidigungslinien in fundamentaler Weise: Denn aus juristischer Sicht bildet das so definierte operative Management bereits die *zweite* Verteidigungslinie, die zur ersten Verteidigungslinie des Verwaltungsrats *hinzutritt*. Demgemäss trägt das operative Management als Verteidigungslinie im integralen Risikomanagement nach schweizerischem Recht die Startnummer 2.

Doch damit nicht genug: Da der Verwaltungsrat gemäss Art. 716a Abs. 1 Ziff. 2 OR die Organisation der Gesellschaft auch mit Blick auf die Anforderungen des integralen Risikomanagements festlegt, hat er die Möglichkeit, weitere Verteidigungslinien für die Aufgabenerfüllung vorzusehen. Entsprechend erfahren nach der juristischen Zählweise auch die weiteren Verteidigungslinien eine numerische Rückstufung: So erhalten nach der zweiten Verteidigungslinie des operativen Managements der Risk Manager/Compliance Manager die *dritte* und der interne Auditor neu die *vierte* Verteidigungslinie zugewiesen.

An dieser Stelle nicht ausser Acht gelassen werden darf zudem die *externe Revisionsstelle,* die durchaus als die fünfte Verteidigungslinie zu bezeichnen ist: Denn für den Verwaltungsrat stellt sie eine wichtige Informationsdrehscheibe, im besten Fall sogar eine Sparringpartnerin, dar. So prüft sie im hier relevanten Kontext bei grösseren Unternehmen namentlich die Existenz des internen Kontrollsystems (IKS) und erstellt einen Review des Lageberichts, der allfällige Widersprüche zwischen dem Lagebericht und der Jahresrechnung aufdecken soll [15]. Die externe Revisionsstelle hält zudem allfällige Mängel des IKS sowie Widersprüche im Lagebericht im Revisionsbericht fest [16].

Und so entwickelt sich aus juristischer Perspektive das etablierte Three-Lines-of-Defense-Modell zum helvetisierten Modell mit fünf Verteidigungslinien weiter, oder eben: zum neuen Five-Lines-of-Defense-Modell.

5. FAZIT

In Übereinstimmung mit der internationalen Best Practice hat der Verwaltungsrat aufgrund seiner Oberleitungspflicht von Gesetzes wegen sicherzustellen, dass er das integrale Risikomanagement des Unternehmens sorgfältig ausgestaltet, implementiert und überwacht (Art. 716a Abs. 1 Ziff. 1 OR).

Jede Nummerierung der mehreren möglichen Lines of Defense beginnt nach schweizerischem Recht deshalb beim Verwaltungsrat als der ersten Verteidigungslinie. Dies bleibt auch dann so, wenn er die Geschäftsführung delegiert: Der Verwaltungsrat verbleibt in der Verantwortung für seine Führungsentscheide, und es tritt die Geschäftsleitung zusammen mit den jeweiligen Risikoeignern als die zweite Verteidigungslinie zu dieser ersten Verteidigungslinie hinzu – allenfalls ergänzt um einen Risikomanager als dritte Verteidigungslinie, einen internen Revisor als vierte und die externe Revisionsstelle als fünfte Verteidigungslinie. Im voll ausgebauten Five-Lines-of-Defense-Modell orchestriert der Verwaltungsrat somit insgesamt bis zu fünf Verteidigungslinien, einschliesslich sich selbst.

In führungsmässiger Hinsicht bleibt anzumerken, dass die besondere Herausforderung für den Verwaltungsrat als dem Oberleiter der Gesellschaft darin liegt, aus den bis zu fünf möglichen Verteidigungslinien osmotisch miteinander kommunizierende Gefässe zu formen, wenn er den eigentlichen Zweck des integralen Risikomanagements erreichen will: nämlich das ihm zur Führung anvertraute Unternehmen resilienter, widerständiger, gegen die Unbill der Zeit zu machen. ■

Anmerkungen: 1) Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006. **2)** Vgl. FERMA/ECIIA, Guidance on the 8th EU Company Law Directive, Article 41, Brüssel, 2010; IIA, Position Paper: The Three Lines of Defense in Effective Risk Management and Control, Altamonte Springs, 2013. **3)** IIA, Anm. 2, S. 2. **4)** Der Begriff Geschäftsführung ist gesetzlich nicht definiert. Gemäss Lehre und Rechtsprechung fallen darunter «sämtliche auf die Verfolgung des Gesellschaftszweckes gerichteten Tätigkeiten» (Watter, R., Roth Pellanda, K., Art. 716 N 9, in: Honsell, H., Vogt, N. P., Watter, R., (Hrsg.), Basler Kommentar, Obligationenrecht II, 5. Auflage, Basel 2016). **5)** Das Three-Lines-of-Defense-Modell wird momentan überarbeitet. Es soll inskünftig flexibler adaptierbar und auch auf kleinere Unternehmen anwendbar sein. **6)** Vgl. zum Ganzen Durrer, M., Die Pflicht des Verwaltungsrates zum integralen Risikomanagement in KMU, Dissertation, Zürich 2017, S. 29 ff. **7)** Durrer, Anm. 6, S. 29 ff. **8)** Vgl. zum Ganzen Böckli, P., Schweizer Aktienrecht, 4. Aufl., Zürich 2009, N 303a zu § 13. **9)** Durrer, Anm. 6, S. 59 ff. **10)** Durrer, Anm. 6, S. 310. **11)** Mittlerweile stellen auch die neuesten Versionen von ISO 31000 und COSO ERM zusätzlich auf die Werte, die Vision und die Mission einer Organisation ab. **12)** Die Risikopolitik legt den Umgang mit Risiken im Unternehmen fest und vereinheitlicht diese. Sie enthält namentlich die Risikomanagementziele, die Risikomanagementstrategie zur Zielerreichung sowie den Risikoappetit des Unternehmens, also dessen Risikobereitschaft. **13)** Die Risikokultur bildet sich aus dem Denken und Handeln aller Mitarbeitenden sowie durch das Vorleben des Verwaltungsrats (Tone at the Top). In der Risikokultur zeigt sich, inwiefern die Risikopolitik im Unternehmen umgesetzt wird. Dabei kann ein Verhaltenskodex helfen, akzeptierte und nicht akzeptierte Verhaltensweisen festzulegen. **14)** «The inputs to risk management are based on historical and current information, as well as on future expectations.» (ISO 31000:2018, Risk management – Guidelines, S. 3). **15)** Neuhaus, M., Inauen, B., Art. 961c N 4 OR, in: Honsell, H., Vogt, N. P., Watter, R. (Hrsg.), Basler Kommentar, Obligationenrecht II, 5. Auflage, Basel 2016. **16)** Neuhaus, Inauen, Anm. 15; Pfiffner, D., Watter, R., Art. 728b N 4 OR, in: Honsell, H., Vogt, N. P., Watter, R. (Hrsg.), Basler Kommentar, Obligationenrecht II, 5. Auflage, Basel 2016.