SO GELINGT DAS RISIKOMANAGEMENT

Auch ohne explizite Pflicht müssen KMU und Behörden in der Schweiz ihre Risiken managen, sonst haften die Verantwortlichen unter Umständen persönlich. Im Artikel erklärt der Autor, was das genau heisst und wie Risikomanagement sinnvoll und pragmatisch angepackt werden kann.

- **Von Christian Hafner**

Einleitung

Immer mehr Verwaltungsräte und Behörden erkennen, dass

- die grössten Risiken wie Verlust des guten Namens oder Cyber-Gefahren nicht oder nur unzureichend versichert werden können und
- es notwendig ist, Risiken nachweisbar zu managen, um die gesetzliche Prüfungs- und Handlungspflicht zu erfüllen.

Die Erkenntnis ist das eine. Zur Tat zu schreiten, ist das andere. In diesem Sinne sollen die nachfolgenden Ausführungen aufzeigen, dass Risikomanagement für KMU und Behörden heutzutage ein Muss ist und pragmatisch umgesetzt werden kann. Schliesslich übersteigt der Nutzen eines RMS, wenn richtig angepackt, das Management der Gefahren und schliesst die Chancen mit ein. Denn wo es Gefahren gibt, gibt es immer auch Chancen.

Die gesetzliche Pflicht zum Risikomanagement

Durch die OR-Revision im Jahr 2013 müssen nur noch «grössere Unternehmen» im Lagebericht Aufschluss über die Durchführung einer Risikobeurteilung geben. Diese Berichterstattungspflicht entfällt für KMU, die nicht ordentlich geprüft werden müssen.

• HINWEIS

Kommt der VR der Risikomanagementpflicht nicht nach, droht ihm unter Umständen eine aktienrechtliche Verantwortlichkeitsklage oder möglicherweise eine strafrechtliche Verfolgung.

Damit wurde die Prüfungspflicht[1] des unternehmensinternen Risikomanagements für KMU-Verwaltungsräte aber nicht aufgehoben. Diese gesetzliche **Prüfungspflicht** ist völlig grössenunabhängig. Zudem unterliegen die Unternehmensführung und der Verwaltungsrat der Pflicht, den Risiken durch aktives *Handeln* zu begegnen.

Implizit sind die Leitungsorgane in der Schweiz gesetzlich verpflichtet, ein Risikomanagementsystem zu betreiben, denn

- *prüfen* kann nur, wer die Risiken des Unternehmens identifiziert, analysiert und bewertet.
- *handeln* kann nur, wer das Risikomanagement sowie das interne Kontrollsystem aktiv ausgestaltet, implementiert und überwacht.

Risiken versichern anstatt managen

Risiken versichern tönt nach einem eleganten Ausweg, um selbst nicht aktiv Risiken managen zu müssen. Der Haken dabei ist, dass das Abwälzen von Risiken nur eine mögliche Strategie ist. Sie muss deshalb nicht immer die richtige und beste sein.

• TIPP

Für jedes Risiko gilt es zu prüfen, ob es abgewälzt, akzeptiert, begrenzt, vermieden oder vermindert werden soll und kann. Mit einer Versicherung kann das Risiko nur teilweise abgewälzt werden.

1 Pflicht aufgrund der gesetzlichen, unübertragbaren und unentziehbaren Verantwortung der Überwachung des Unternehmens von Gesetzes wegen (Art. 716a OR).

Nehmen wir als Beispiel die Cyber-Gefahr – gemäss dem Allianz Risk Barometer das Top-Risiko 2022 in der Schweiz mit 61% Nennungen. Besonders «doppelte Erpressungstaktiken» sind ein besorgniserregendes Cyber-Risiko.

Immer öfter beschränken sich Cyber-Kriminelle nicht nur auf das Erpressen von Lösegeld nach Verschlüsselung von Daten. Sie drohen nachfolgend auch mit Veröffentlichung sensibler Daten, wenn nicht nochmals gezahlt wird. Somit löst der Eintritt eines Cyber-Risikos sofort auch ein **Reputationsrisiko** aus. Der Verlust des guten Namens kann aber nicht versichert werden. Dasselbe gilt für viele andere Risiken, wie zum Beispiel bei der Verletzung von Nachhaltigkeitsverpflichtungen. Deshalb bleibt nur: Selbst vorsorgen!

Selbst wenn Sie eine Cyber-Schutz-Versicherung abschliessen, ist diese Abwälzungsstrategie nicht genügend. Die Auswirkungen bei Einritt des Risikos sind so schlimm, dass Sie Ihrer Verantwortung nur gerecht werden, wenn Sie (zusätzlich) andere Risikostrategien anwenden.

Das Reputationsrisiko gilt als das bedeutsamste und gleichzeitig am schwierigsten zu handhabende Risiko. Umso mehr sollten die Ursache- und Wirkungsbeziehungen zwischen Reputationsrisiken und anderen Risikoarten umfassend analysiert werden. Nur so können Reputationsrisiken möglichst überschneidungsfrei identifiziert und gesteuert werden.

Einstieg ins Risikomanagement leicht gemacht

Der Einstieg ins Risikomanagement gelingt am besten mit einem pragmatischen Ansatz. Wenn richtig gemacht, eröffnet das Vorgehen erst noch Chancen, die geschäftlich genutzt werden können.

Risikomanagement ist im Grunde weder kompliziert noch aufwendig. Zudem ist es nichts Neues. Es wurde schon immer praktiziert. Es hiess einfach anders: Vorbeugungsmassnahmen. Ein Risiko (möglicher Fehler) wurde gefunden, die Ursache ermittelt, Massnahmen ergriffen.

Das gehört zum Tagesgeschäft jedes Unternehmers und Geschäftsführers und jeder Unternehmerin und Geschäftsführerin. Sie kommen morgens ins Unternehmen und sehen **Risiken und Chancen.** Dann treffen sie Entscheidungen und Massnahmen, um die Risiken zu vermeiden und um die Chancen nutzen zu können.

Was sich verändert hat, ist das Bewusst- und Transparentmachen dieses Verhaltens. Die Entscheidungen, welche zu den Vorbeugungsmassnahmen führen, werden im Risikomanagement bewusst getroffen und transparent kommuniziert. Zudem wird die Wirksamkeit der Entscheidungen überprüft, und diese Resultate dienen der Überprüfung der Entscheidungen – und all das in einer angemessenen Häufigkeit.

Praxistipp 1: Ermittlung von Chancen und Risiken

Die übliche Methodik zur Ermittlung von Chancen und Risiken war einem meiner Kunden zu abstrakt.

Deshalb haben wir damit begonnen, dass er einfach mal auf das vergangene Jahr zurückschaut und sich vor Augen führt, was er am oder im Unternehmen verändert hat. Der Grund für Veränderungen ist oft eine Chance oder ein Risiko, welches man gesehen hat. Das war einem zum damaligen Zeitpunkt vielleicht nicht so abstrakt bewusst. Dieser Rückblick machte meinen Kunden sensibler für die Chancen und Risiken und die diesbezüglichen Massnahmen in der Gegenwart.

Praxistipp 2: Risikobeurteilung mit Blick auf die Herkunft der Profite

Die Risiko-Heatmap eignet sich zum Management der groben Risiken. Aber wie die Risikoelemente im Griff behalten, welche direkt die Rentabilität bedrohen?

Bei diesem Ansatz ist der Ausgangspunkt für die Risikoanalyse die Gewinnlandschaft – nicht ihre potenziellen Risiken. Wenn 20% Ihrer Kundschaft und Produkte 150% oder mehr Ihres Gewinns erwirtschaften, ist der wichtigste Aspekt des Risikomanagements der Schutz und das Wachstum dieser Gewinnbeiträge.

Der Kern des Risikomanagementprozesses ist eine sorgfältige Analyse, welche Kundinnen und Kunden und Produkte zum Segment mit den hohen Gewinnbeiträgen gehören und was deren Profitabilität gefährdet oder steigern würde.

Die wichtigste Risikosteuerungsmassnahme ist deshalb die genaue und kontinuierliche Überwachung der Gewinneinbussen oder des Gewinnwachstums jeder einzelnen Kundin/jedes einzelnen Kunden und Produkts in den «Gewinnspitzen». Dazu gehört eine sorgfältige regelmässige Überprüfung externer oder interner Bedrohungen, die sich speziell auf dieses Segment beziehen.

Auch wenn der Einstieg ins Risikomanagement für alle KMU und Behörden geboten ist, ohne dass zwei Voraussetzungen erfüllt sind, lohnt sich der Aufwand nicht.

1. **Engagement der Führung**
   Die oberste Führungsebene will tatsächlich ein wirksames Risikomanagement, damit die «richtigen» Risiken eingegangen werden.

2. **Rollen und Verantwortlichkeiten**
   Es besteht der Wille zur klaren Formulierung von Verantwortlichkeiten für das Risikomanagement auf allen Ebenen. Geeignete personelle Ressourcen zur Übernahme der Rollen und Verantwortlichkeiten sind vorhanden, oder es besteht die Bereitschaft, sie zu beschaffen.

IKS braucht Risikomanagement

Bis vor Kurzem konnte man der Auffassung sein, dass, wer ein IKS betreibt, kein Risikomanagementsystem braucht. In Lehre und Praxis wurde organisatorisch klar zwischen beiden unterschieden. Das hat sich geändert. Das einflussreiche «Institute of Internal Auditors (IIA)» empfiehlt, diese Trennung aufzugeben, und hat dazu im Juli 2020 ein Update zum Drei-Linien-Modell publiziert.[2]

• HINWEIS

Das IKS und Risikomanagement sind nicht (mehr) zwei getrennte Disziplinen. Das oberste Leitungsorgan ist für beides verantwortlich.

Das (oberste) Leitungsorgan bestimmt die Risikobereitschaft der Organisation und übt die Aufsicht über das Risikomanagement (inkl. der internen Kontrollen) aus. Als interne Kontrollen werden die Prozesse bezeichnet, die sich zur Schaffung angemessenen Vertrauens zur Erreichung der Ziele eignen.

2 Quelle: Deutsches Institut für Interne Revision, IIA Positionspapier: Das Drei-Linien-Modell. Es kann davon ausgegangen werden, dass das COSO* dieses Drei-Linien-Modell vom IIA wie bis anhin übernehmen wird. *Committee of Sponsoring Organizations of the Treadway Commission (Platform established 1985 for the US National Commission on Fraudulent Financial Reporting).

Das Management

- errichtet und unterhält geeignete Strukturen und Prozesse für das Management des Betriebs und der Risiken (inkl. interner Kontrollen).
- entwickelt, implementiert und verbessert kontinuierlich die Risikomanagementpraktiken (inkl. interner Kontrollen) auf Prozess-, System- und Entitätsebene.
- stellt das Erreichen der Risikomanagementziele sicher, wie z.B. Einhaltung von Gesetzen, Regulierungen und akzeptablem ethischem Verhalten, interne Kontrollen, Informations- und Technologiesicherheit, Nachhaltigkeit und Qualitätssicherung.
- stellt Analysen und Berichte über die Angemessenheit und Wirksamkeit des Risikomanagements (inkl. interner Kontrollen) bereit.

Das (oberste) Leitungsorgan, der Verwaltungsrat, die Behörde

- ist für die Ausgestaltung, Implementierung und Aufrechterhaltung einer geeigneten und angemessenen internen Steuerung und Kontrolle verantwortlich.
- sorgt für ein dem Unternehmen angepasstes Risikomanagement und ein internes Kontrollsystem.

Risikomanagement braucht Hinweisgeberschutz

Allen, die bereits ein Risikomanagement etabliert haben, empfehle ich eine zusätzliche Überlegung. Studien und Erfahrungen zeigen, dass ein grosser Teil des Fehlverhaltens der betroffenen Organisation durch Meldungen von Personen innerhalb oder in der Nähe der Organisation zur Kenntnis gelangen. Obwohl in der Schweiz nicht gesetzlich vorgeschrieben, lohnt sich aus der Perspektive des Risikomanagements der Betrieb eines **Hinweisgebersystems.** Bei Organisationen mit funktionierendem Meldesystem werden bis zu 80% der Missstände durch Hinweisgeber aufgedeckt. Schon im Oktober 2007 schrieb die Eidgenössische Finanzkontrolle in Ihrer Broschüre «Aufbau eines IKS» auf Seite 11: *«[…] sowie eine Anlaufstelle für Informationen betreffend möglicher Unregelmässigkeiten (Whistleblowing), können die Effizienz von Kontrollsystemen spürbar erhöhen.»*

• TIPP

Wer wirkungsvoll Risiken managen will, muss für den Schutz der Hinweisgeber sorgen. Interne Kontrollen allein genügen nicht.

Tatsächlich führt Whistleblowing nicht selten zur Entdeckung sog. **Innentäter.** Da die Täter/-innen oft bis zur Entdeckung nicht von ihrem kriminellen Tun ablassen, wird der Schaden umso grösser, je länger sie unentdeckt bleiben. Und da kriminelle Energie im Spiel ist, finden die Täter/-innen auch Mittel und Wege, die herkömmlichen Kontrollsysteme zu überlisten. Deshalb zeigt sich gerade hier – unabhängig von einer gesetzlichen Verpflichtung – der grosse Mehrwert von Hinweisgebersystemen für Unternehmen und Organisationen. Die Einführung eines Hinweisgebersystems hat einen abschreckenden Effekt. Die Statistiken zur Untermauerung dieser These stammen zwar aus dem Finanzsektor. Die Forscher sind sich aber einig, dass es sich bei den identifizierten Effekten des Whistleblowings nicht um ein reines Finanzmarktphänomen handelt.

Anstelle eines Schlussworts

Wenn Sie sich zum Thema Risikomanagement umhören und mit Experten sprechen, stossen Sie schnell auf den Begriff GRC.

GRC-Konzepte geben vor, «Governance», «Risk» und «Compliance» miteinander zu verknüpfen und so integrativ das Risikomanagement betreiben zu können.

• TIPP

GRC-Konzepte genügen nicht für die Umsetzung eines unternehmerischen Risikomanagements, weil der Risikobegriff in GRC die Chancen ausschliesst.

Da in der Praxis bei der Umsetzung schliesslich leider oft die «Compliance-Perspektive» dominiert, wird Risiko lediglich als Gefahr verstanden und nur das Ziel verfolgt, Risiken zu vermeiden bzw. zu minimieren. Compliance-Officer gehen sogar noch weiter und sehen ein Risiko als Fehler (Wenn sie der verlängerte Arm der Aufsichtsbehörde sind, sind sie gezwungen, diese Sicht anzunehmen.) Ein derartiges Risikoverständnis und die damit verbundene Risikokultur widersprechen einer unternehmerischen Sicht von Risiko diametral. Eine unternehmerische Risikokultur akzeptiert, dass jede unternehmerische Tätigkeit – und jede unternehmerische Entscheidung – immer mit Chancen und Gefahren (Risiken) verbunden ist. Für Entscheidungen müssen die damit verbundenen Gefahren und Chancen betrachtet werden. Unternehmerisch betrachtet bedeutet **Risiko = Chance und Gefahr.** Somit ist klar, dass das Eingehen von Risiken nicht grundsätzlich einen Fehler darstellt und deshalb selbst die Minimierung von Risiken nicht immer sinnvoll ist. Unternehmerisch entscheiden heisst, Rendite und Risiko zu optimieren.

• HINWEIS

Lassen Sie die Compliance-Perspektive nicht dominieren. Wenn Risiko nur als Gefahr verstanden und minimiert werden muss, können Risikobeurteilungen nicht adäquat in unternehmerische Entscheide einfliessen.

AUTOR
Christian Hafner ist Finance- und Governance-Experte. Er setzt RM- und IKS-Projekte für KMU und Gemeinden um.