Integrales Risikomanagement für KMU

Jede Geschäftstätigkeit ist mit Risiken und Gefahren verbunden. Es gibt unzählige Führungssysteme, um diese präventiv zu managen oder bei Eintritt eines Ereignisses korrekt zu reagieren. Um Aufwand und Nutzen zu optimieren, empfiehlt sich für KMU ein integraler Ansatz, mit welchem Synergien genutzt und Doppelspurigkeiten beseitigt werden.

Von Uwe Müller-Gauss und Madeleine Renner

Die Themen Geschäftskontinuitätsmanagement (engl. Business Continuity Management, BCM), Krisenmanagement (engl. Crisis Management), Risikomanagement (engl. Risk Management, RM) und Internes Kontrollsystem (IKS, engl. Internal Control System) haben an Bedeutung gewonnen. Mängel in diesen Bereichen haben in den letzten Jahren zu diversen Skandalen, Krisen und Unternehmenszusammenbrüchen geführt. Inhaber, Investoren, Gläubiger und Mitarbeitende erlitten grosse finanzielle Schäden und Reputationsverluste. Weltweit wurden nationale und internationale Anstrengungen zur verstärkten Regulierung der Unternehmensführung (Corporate Governance) unternommen. Damit wurden die Interne Kontrolle und das Risikomanagement in vielen Ländern Gegenstand staatlicher Regulierungen.

Die Schweiz hat der internationalen Entwicklung mit der Teilrevision des Revisionsrechts im Jahr 2010 Rechnung getragen. Allerdings ist nur das Ausmass der gesetzlichen Verankerung neu. Im Schweizer Gesellschaftsrecht ist festgehalten, dass die Pflicht und somit die Verantwortung für eine sorgfältige Geschäftsführung beim Leitungsorgan einer Unternehmung liegt. Zu den Pflichten gehören insbesondere Tätigkeiten, welche die langfristige Sicherung der Geschäftstätigkeit sicherstellen wie beispielsweise das Risikomanagement oder das IKS.

Auch aus betriebswirtschaftlicher Sicht ist es zwingend erforderlich, sich mit existenzsichernden Massnahmen und Instrumenten auseinanderzusetzen: einerseits präventiv, um Schäden vorzubeugen und andererseits, um bei Eintritt von «zufälligen» oder unbeachteten Unglücks- und Störfällen die Existenz der Unternehmen zu sichern. Die Globalisierung und die sich kontinuierlich verändernden Rahmenbedingungen – insbesondere in technologischer, wirtschaftlicher und politischer Hinsicht – führen dazu, dass auf ein bewusstes und organisatorisches Risikomanagement kaum mehr verzichtet werden kann. Angesichts dessen, was auf dem Spiel steht, wird die bewusste, systematische und permanente Auseinandersetzung mit den Risiken der Unternehmung zu einer ergänzenden Führungsfunktion, die von der Unternehmensspitze wahrgenommen werden muss. Ziel ist es sicherzustellen, dass die Risiken erkannt und beurteilt werden. Anschliessend wird festgelegt, wie diese bewältigt werden.

Risikomanagement – kontrollierter und bewusster Umgang

Im Rahmen des Risikomanagements sollen Gefahren vermieden werden, welche die Kontinuität des Geschäftsganges und somit den nachhaltigen Fortbestand des Unternehmens, Teile davon oder Projekte gefährden könnten. Das Risikomanagement umfasst alle Tätigkeiten, die der

Identifikation, Bewertung, Bewältigung und Überwachung der wesentlichen Risiken dienen.

Grundlage des Risikomanagements ist das Formulieren einer rationalen und klar umschriebenen Risikopolitik, welche einen Bestandteil der Unternehmenspolitik darstellen sollte. Sie ist darauf ausgerichtet, den Sicherheitsgedanken in den Unternehmungsentscheidungen durchgängig zu berücksichtigen und damit auch die Leitziele des Risikomanagements auf operationeller Stufe festzulegen. Nur wer eine umfassende und systematische Risikopolitik betreibt, ist in der Lage, in Kenntnis aller Umstände und damit bewusst risikofreudig zu sein, wo dies nötig und angebracht ist und auch verantwortet werden kann. Des Weiteren braucht es organisatorische Massnahmen wie die Definition von Prozessen, Aufgaben, Zuständigkeiten und Verantwortung.

Im Rahmen der Risikoidentifikation wird analysiert, welche externen oder internen Gefahren die Erreichung der Strategie respektive Unternehmensziele verhindern könnten. Anhand von Hilfsmitteln wie Checklisten, Prozess- und Gefährdungsanalysen, Workshops etc. wird versucht, die wesentlichen Risiken zu identifizieren. Aus dieser Klärung resultiert oft ein Risikokatalog. Im Rahmen der Risikoanalyse werden die identifizierten Risiken analysiert und bewertet.

Die Bewertung kann mit unterschiedlichen Methoden vorgenommen werden. Weitverbreitet ist die Berechnung nach Eintrittswahrscheinlichkeit multipliziert mit Schadensausmass. Die Eintrittswahrscheinlichkeit ist jedoch meist schwer zu berechnen und bedeutet eine realitätsfremde Vereinfachung. Deshalb bewerten nachhaltige Risikomanager die Risiken mit den folgenden Metriken:

- Schadensausmass qualitativ von «kein Schaden» bis «sehr hohe Auswirkung/Marktanteilsverlust» (I1)
- Schadensausmass quantitativ z.B. von «50 000 bis >1 000 000» oder «%-Anteil vom Eigenkapital» etc. (I2)
- Entwicklungszeit/Dauer bis zum Erkennen des Ereignisses von «sofort/zwingend» bis «keine Entdeckung» (A1)
- Umgang im Ereignisfall/Ereignisbewältigung von «integriertes Krisenmanagement» bis «keine Mechanismen» (A2)
- Kontrolle bei Risikoexposition von «volle Kontrolle» bis «keine Kontrolle» (T1)
- Bewusstsein, Sensibilisierung für die Risikoexposition von «volles Bewusstsein» bis «unbekannt/nicht bewusst» (T2)

Risiko-Nr.	Risiko-Bezeichnung	Bereich	
17	Verletzung des Datenschutzes: Schnittstellen (durch externe – Verpflichtungserklärungen)	Strategische Risiken	
Risikobeschreibung			
Sensible Daten gelangen an Unberechtigte bzw. werden missbraucht.			
Metrik		Bewertung gemäss Workshop	Priorität
I1	Schadenausmass qualitativ	hohe Aussenwirkung und deutliche Störungen	4
I2	Schadenausmass quantitativ in CHF	bis 500.000 CHF	3
A1	Entdeckungszeit	lang/ zufällig	4
A2	Umgang im Ereignisfall	integriertes Krisenmanagement	1
T1	Kontrolle	eher gut/ direkt	2
T2	Bewusstsein	hoch	2

Metriken der Risikobewältigung (nach Uwe Müller-Gauss)

Für Risiken, welche bewusst eingegangen werden, werden im Rahmen der **Risikosteuerung** Massnahmen eruiert und definiert, welche das Risiko auf das gewünschte Niveau reduzieren sollen. Die Einteilung in sechs Metriken erlaubt eine feine und gezielte Steuerung des Risikos.

IKS – ordnungsmässige und effiziente Geschäftsführung

Ziele des IKS sind, eine ordnungsmässige und effiziente Geschäftsführung zu gewähren, das Vermögen und die Zuverlässigkeit des Rechnungs- und Berichtswesens sicherzustellen sowie die Einhaltung der unternehmerischen Ziele, Gesetze, Weisungen und Vorschriften zu unterstützen.

Es empfiehlt sich, ein IKS-Konzept zu erstellen, in welchem die Unternehmensleitung den gewünschte Umfang und

ERFOLGSFAKTOREN FÜR KMU IM BEREICH RISIKOMANAGEMENT

- Rationale und klar umschriebene d.h. schriftlich festgehaltene Risikopolitik
- Klare Regelungen der Aufgaben, Kompetenzen und Verantwortlichkeiten
- Betrachtung des Risikomanagements als Daueraufgabe und nie als abgeschlossenen Prozess
- Das RM ist den Mitarbeitenden bekannt und wird aktiv gelebt
- Eine nachhaltige Bewertung und Steuerung der Risiken nach unternehmensspezifischen Metriken
- Integration mit anderen Instrumenten (IKS, Krisenmanagement, BCM)

ERFOLGSFAKTOREN FÜR KMU IM BEREICH IKS

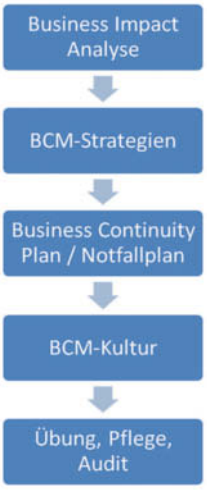
- Klare und realistische Festlegung der Ziele und der angestrebten Qualität
- Ausrichtung der Kontrollen auf die Unternehmensziele und die Risiken, welche die Erreichung der Unternehmensziele gefährden können
- Klare Regelungen der Aufgaben, Kompetenzen und Verantwortlichkeiten
- Das IKS ist den Mitarbeitenden bekannt und wird aktiv gelebt
- Kein ausschliesslicher Fokus auf die finanzielle Berichterstattung (Financial Reporting), sondern auch Beachtung der Felder «Wirksamkeit und Effizienz der Geschäftstätigkeit (Operations)» und «Gesetzes- und Normenkonformität (Compliance)»
- Integration mit anderen Instrumenten (RM, Krisenmanagement, BCM)

Ausbaugrad sowie die Qualität (wenig verlässlich bis optimiert) des IKS strategisch festlegt, Ziele formuliert und Kriterien für die Beurteilung der Qualität der Kontrollen festlegt sowie die Aufgaben und Verantwortlichkeiten regelt. Weitere wichtige Grundlagen sind die Dokumentationen der wesentlichen Unternehmensprozesse und eine Aufstellung der bestehenden Kontrollen. Auch wenn ein Unternehmen noch kein systematisches IKS unterhält, hat es bereits eine Vielzahl von Kontrollen wie z.B. die Kollektivunterschrift, Vier-Augen-Prinzip, Funktionentrennungen, Zugriffs- und Zutrittsbeschränkungen etc. Durch eine systematische Aufnahme der Istsituation können Doppelspurigkeiten und Kontrollücken aufgedeckt werden. Meist führt dies zu einer Optimierung der Geschäftsprozesse. Anschliessend wird eine Risikobeurteilung vorgenommen – denn es gilt der Grundsatz: Ohne Risiko braucht es keine Kontrolle. Dabei werden die Risiken identifiziert und bewertet.

BCM – Bewältigung des Restrisikos

Mit einem Business Continuity Management (BCM) soll sichergestellt werden, dass die «lebensnotwendigen» Aktivitäten eines Unternehmens nach internen oder externen Ereignissen aufrechterhalten resp. zeitgerecht wiederhergestellt werden und finanzielle sowie reputative Folgeschäden minimiert werden können.

Die hier verwendete Methode zum Aufbau und der Implementierung eines BCM richtet sich nach den aktuellen Standards und Guidelines des Business Continuity Instituts (BCI, London). Die Methode besteht grundsätzlich aus einer wiederkehrenden Abfolge von fünf Phasen, welche von der Analyse des eigenen Geschäfts (Phase 1) bis hin zur regelmässigen Pflege des aufgebauten BCM reicht.



Hauptbestandteil der ersten Phase bildet zusammen mit einem Risk Assessment die sogenannte Business Impact Analysis (BIA). Mit dieser Analyse werden die kritischen Aktivitäten und Prozesse eines Unternehmens ermittelt. Die BIA ist das Rückgrat des BCM, weil aus den generierten Resultaten die Strategien entwickelt werden (Phase 2), mit denen ein Unternehmen auf den Unterbruch oder die Störung einer kritischen Aktivität reagieren will. Die BIA und die Entwicklung von BCM-Strategien werden von der EBK als verbindlicher, aufsichtsrechtlicher Mindeststandard und gemäss Art. 3 des BankG als Bewilligungsvoraussetzung zum Geschäftsbetrieb erachtet.

In Phase 3 werden Reaktionen, sogenannte Business Continuity Plans (Notfallpläne), im Hinblick auf einen Unterbruch einer kritischen Geschäftsaktivität entwickelt. Diese Pläne dokumentieren die Vorgehensweisen im Falle eines Ereignisses und bestimmen die Ressourcen, die notwendig sind, um die unterbrochenen Aktivitäten wiederherzustellen.

Um das BCM im Unternehmen zu verankern, muss das Bewusstsein der Mitarbeitenden für die Notwendigkeit eines BCM geschaffen und geschult werden (BCM-Kultur) (Phase 4).

In Phase 5 werden die Komponenten des BCM getestet und geübt, weil sich ein Unternehmen ständig verändert. Tests und Übungen identifizieren Schwachstellen des BCM und ermöglichen Anpassungen.

Krisenmanagement – handlungs- und entscheidungsfähig bleiben

Das Krisenmanagement dient zur Bewältigung ausserordentlicher Ereignisse. Es soll sicherstellen, dass im Ereignisfall durch zeitgerechte und gezielte Massnahmen der Schutz der Mitarbeitenden gewährleistet werden kann und Schäden an Vermögenswerten und dazugehörige Folgeschäden auf eine Minimum begrenzt werden können.

Das Krisenmanagement verfolgt die folgenden Ziele:

- Schadensbegrenzung (Mitarbeitende, Betrieb, Dritte)
- Aufrechterhaltung bzw. Wiederherstellung der wichtigsten Betriebsabläufe
- Zeitgerechte, aktive, transparente und verlässliche, auf die Zielgruppen ausgerichtete interne und externe Kommunikation (Schutz des Rufes der Unternehmung als glaubwürdiges Unternehmen)
- Rasche Wiederherstellung des Normalzustandes

Die Bewältigung von Krisenfällen erfordert eine Organisationsform und Führungsstrukturen, die sehr rasch – auch ausserhalb der Bürozeiten – funktionstüchtig sind

- eine klare, auf die ausserordentliche Lage abgestimmte Aufgabenabgrenzung vorsehen

ERFOLGSFAKTOREN FÜR KMU IM BEREICH BCM

- Die kritischen Prozesse sind bekannt
- Eine Überlebensstrategie garantiert den Fortbestand
- Notfallpläne helfen bei einem schnellen Wiederanlauf resp. Notbetrieb
- Schnellstmögliche Wiederherstellung des Normalbetriebs ist möglich
- Integration mit anderen Instrumenten (RM, IKS, Krisenmanagement)

ERFOLGSFAKTOREN FÜR KMU IM BEREICH KRISENMANAGEMENT

– Bewältigung von ausserordentlichen Ereignissen mit eigenen und fremden Ressourcen
– Kommunikations-Lead sicherstellen
– Schaden eingrenzen und schnellstmöglich beheben
– Auch in der Krise handlungs- und entscheidungsfähig bleiben
– Integration mit anderen Instrumenten (RM, IKS, BCM)

– Entscheidungen in kurzer Frist ermöglichen
– Sonderkompetenzen für die zeitgerechte Anordnung von Massnahmen beinhalten
– frei sind von Prestigedenken und Beharren auf Zuständigkeiten aus dem Alltag
– die notwendigen Infrastrukturen zur Verfügung stellen, sodass zielführendes Arbeiten möglich ist und die Infrastrukturen auch dann funktionieren, wenn die im Normalfall verwendeten Mittel ausfallen

Das Krisenmanagement besteht aus folgenden Säulen:

Im **Führungsmanagement** ist ein zum Voraus definierter und geschulter Krisenstab jederzeit abrufbereit. Bei Kriseneintritt nimmt dieser seine Tätigkeit sofort auf. Er ist in der Regel von seinen operativen Tätigkeiten entbunden und verfolgt einzig das Ziel der erfolgreichen Bewältigung der Krise. Der Krisenstab organisiert sich so, dass er jederzeit rasch und unkompliziert Zugang zu den benötigten Informationen hat. Er ist in der Regel am Ort des Geschehens vertreten. Damit er stets handlungsfähig bleibt, muss er sich auch den Informations- und Kommunikationslead sichern. Er wird über wichtige Entwicklungen stets auf dem Laufenden gehalten und ist verantwortlich für die Steuerung der Kommunikation.

Das **Kommunikationsmanagement** dient dazu, dass die Unternehmung mit «einer Stimme» kommuniziert. Kommunikation in Krisen ist Chefsache, er oder sie nimmt in der Öffentlichkeit Stellung. Daneben äussert sich nur der offizielle Mediensprecher oder von ihm autorisierte Fachpersonen zu entsprechenden Fachfragen. ■

UWE MÜLLER-GAUSS
ist Dipl. Entrepreneur FH MBA und Inhaber der MÜLLER-GAUSS CONSULTING in Hinwil. Er ist Dozent an der Hochschule Luzern.

MADELEINE RENNER
ist BSc Business Administration; Management & Law. Wissenschaftliche Mitarbeiterin am Institut für Betriebs- und Regionalökonomie, Competence Center Management & Law der Hochschule Luzern.