DOSSIER
RISIKO & ABSICHERUNG


Bild: Daniel Stricker, pixelio.de

Risikomanagement für KMU: Eine Übersicht. Es bestehen unzählige Führungssysteme, um Risiken präventiv zu managen oder bei Eintritt eines Ereignisses korrekt zu reagieren. Wichtige Instrumente sind das Risikomanagement, das interne Kontrollsystem (IKS), das Krisenmanagement und das Kontinuitätsmanagement (BCM).

VON UWE MÜLLER-GAUSS UND MADELEINE RENNER*

Im Schweizer Gesellschaftsrecht ist festgehalten, dass die Pflicht und somit die Verantwortung für eine sorgfältige Geschäftsführung beim Leitungsorgan einer Unternehmung liegen. Dazu gehören insbesondere Tätigkeiten, welche die langfristige Sicherung der Geschäftstätigkeit sicherstellen wie beispielsweise das Risikomanagement oder das IKS. Auch aus betriebswirtschaftlicher Sicht ist es elementar, 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 nur schwer quantifizierbaren Folgen einer Unterbrechung der Betriebs- oder Leistungsbereitschaft der Unternehmung sind Kunden- und Marktanteilsverluste, die nur ungenügend versicherbar sind. Dieser Artikel stellt die Instrumente Risikomanagement, IKS, Krisenmanagement und BCM vor und zeigt wichtige Erfolgsfaktoren für KMU auf.

Risikomanagement: kontrollierter und bewusster Umgang mit Risiken. 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.

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. Oft resultiert aus

dieser Analyse 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[1]

> 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)

Die Metriken lassen sich den Bedürfnissen des Unternehmens anpassen. Die nachfolgende Abbildung zeigt ein Beispiel eines bewerteten Risikos auf (siehe Grafik). 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. Ziel des Internen Kontrollsystems IKS ist es, eine ordnungsmässige und effiziente Geschäftsführung zu gewähren, das Vermögen und die Zuverlässigkeit des Rechnungs- und Berichtswesen sicherzustellen sowie die Einhaltung der unternehmerischen Ziele, Gesetze, Weisungen und Vorschriften zu unterstützen. Zudem dient es zur Verhinderung bzw. Aufdeckung von deliktischen Handlungen und Fehlern. Es empfiehlt sich, ein **IKS-Konzept** zu erstellen, in welchem die Unternehmensleitung dengewünschten Umfang und Ausbaugrad sowie 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** sowie eine Aufstellung der **bestehenden Kontrollen.** Auch wenn ein Unternehmen noch kein systematisches IKS unterhält, hat es bereits eine Vielzahl von Kontrollen wie z.B. Kollektivunterschrift, Vier-Augen-Prinzip, Funktionentrennungen, Zugriffs- und Zutrittsbeschränkungen etc. Durch eine systematische Aufnahme der Ist-situation können Doppelspurigkeiten und Kontrolllücken 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. Anschliessend werden für die Risiken **Kontrollen definiert** und in einer Übersicht festgehalten.

Business Continuity Management (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). Es hat sich bewährt, die Bankenmethoden auch für andere Branchen zu adaptieren. Die Methode besteht grundsätzlich aus einer wiederkehrenden Abfolge von fünf Phasen.

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 in der zweiten Phase die **Strategien** entwickelt werden, mit denen ein Unternehmen auf den Unterbruch oder die Störung einer kritischen Aktivität reagieren will. In Phase 3 werden Reaktionen, sogenannte Business Continuity Plans **(Notfallpläne),** 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 **beübt.** Tests und Übungen identifizieren Schwachstellen des BCM und ermöglichen Anpassungen.

Risiko-Nr.	Risikobezeichnung	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	Schadensausmass qualitativ	hohe Aussenwirkung und deutliche Störungen	4
I2	Schadensausmass 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: Das Beispiel zeigt, dass bei der langen Entdeckungszeit Handlungsbedarf besteht, jedoch nicht beim Umgang im Ereignisfall.

[1] Diese Methodik wurde von Uwe Müller-Gauss entwickelt.

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 die dazugehörigen Folgeschäden auf eine Minimum begrenzt werden können. Dies erfordert eine Organisationsform und Führungsstrukturen, die

> sehr rasch – auch ausserhalb der Bürozeiten – funktionstüchtig sind
> eine klare, auf die ausserordentliche Lage abgestimmte Aufgabenabgrenzung vorsehen
> 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 auch dann funktionieren, wenn die im Normalfall verwendeten Mittel ausfallen.

Das Krisenmanagement besteht aus den drei Säulen **Führung, Kommunikation** und **Care.** Im Führungsmanagement ist ein zum Voraus definierter und geschulter Krisenstab jederzeit abrufbereit. Der Krisenstab organisiert sich so, dass er jederzeit rasch und unkompliziert Zugang zu den benötigten Informationen hat und ist in der Regel am Ort des Geschehens vertreten. Das Kommunikationsmanagement dient dazu, dass die Unternehmung mit «einer Stimme» kommuniziert. Kommunikation in Krisen ist Chefsache. Mit dem **Care Management** schliesslich wird das Ziel der psychologischen Notfallbetreuung verfolgt. Es geht darin insbesondere um die Bewältigung eines traumatischen Ereignisses durch psychologische Notfallbetreuung sowie langfristig um die Erhaltung der Arbeitsfähigkeit.

*

UWE MÜLLER-GAUSS
ist Inhaber der MÜLLER-GAUSS CONSULTING in Hinwil. Er verfügt über mehrjährige Erfahrung bei der Realisierung von Security-, Risk- & Continuity-Management-Strategien, Sicherheits- und Notfallorganisationen, Sicherheitsprüfungen (Revision) und Führungsinstrumenten für das Krisenmanagement und der Ausweichplanung für sensitive Business-Kernprozesse.
uwe.mueller@gauss-consulting.ch

MADELEINE RENNER
ist Wissenschaftliche Mitarbeiterin am Institut für Betriebs- und Regionalökonomie, Competence Center Management & Law der Hochschule Luzern – Wirtschaft und Co-Leiterin des CAS KMU und Recht. Sie verfügt über Erfahrung in der MEM-Industrie (Maschinen-, Elektro- und Metallindustrie) & Medizinaltechnik sowie in der Beratungsbranche und doziert an unterschiedlichen Weiterbildungsinstituten.

ERFOLGSFAKTOREN FÜR KMU

Risikomanagement
> Rationale und klar umschriebene d.h. schriftlich festgehaltene Risikopolitik.
> Klare Regelungen der Aufgaben, Kompetenzen und Verantwortlichkeiten.
> Betrachtung des Risikomanagements als Daueraufgabe und nie 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).

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).

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).

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).

KTI-FORSCHUNGSPROJEKT

«Integrales Risk Management zur ganzheitlichen Sicherung der Geschäftstätigkeit»
Für kleine und mittlere Unternehmen stellt sich Risikomanagement oft als unübersichtliche Ansammlung von Konzepten und Instrumenten dar. Die vier Themenfelder Risikomanagement, Business Continuity Management, Krisenmanagement und das Interne Kontrollsystem werden von KMU vielfach als separate Themenfelder behandelt. Ziel ist die Entwicklung eines Instrumentariums für KMU, das die vier Themenfelder vereint. Das Projekt realisiert die Hochschule Luzern zusammen mit Thomson Reuters, dem Fachverein BCMnet.CH sowie der Beratungsunternehmung RFM Dr. Imfeld und läuft bis im Frühjahr 2014. Das Projekt wird durch die Kommission für Technologie und Innovation KTI der Schweizerischen Eidgenossenschaft mitfinanziert. Im Rahmen des Projektes finden verschiedene Veranstaltungen und ein Workshop statt. Interessierte finden weitere Informationen unter: **www.hslu.ch/integrales-rm**

Knowing. **Not guessing.**

20 Jahre Erfahrung in den Bereichen

PRÄVENTION - RESILIENCE

Bauherrenberatung/ Projektmanagement
Sicherheitsplanung/ Trouble-Shooting
Integrale Tests/ Security & Risk Audits/ Reviews
Risikoanalysen/ Risikomanagement Systeme

EREIGNISBEWÄLTIGUNG - BCM

Business Impact Analysen/ Überlebensstrategien
Business Continuity Management Manuals
Notfall- und Evakuierungskonzepte/ Notfallpläne
Krisenmanagement Handbücher
Krisenstabs- und Evakuierungsübungen

**Es ist besser, beizeiten Dämme zu bauen,
als auf die Vernunft der Flut zu hoffen!**

MÜLLER
GAUSS
CONSULTING

MÜLLER-GAUSS CONSULTING
Security | Risk | Crisis | Continuity Management

+41 44 938 05 04 ● uwe.mueller@gauss-consulting.ch ● www.gauss-consulting.ch