alpha markets
Gesellschaft für
Strategieberatung mbh

Enterprise Risk Management für kleine und mittlere Unternehmen: Ansatzpunkte für eine pragmatische Lösung

Von Stefan Hock, Managing Partner, Uwe Wortmann, Partner, alpha markets Gesellschaft für Strategieberatung mbH, Gauting

Seit einiger Zeit wird erneut unter dem Stichwort "Basel" die Situation der Kreditvergabe an und der Verfügbarkeit von Kapital für kleine und mittlere Unternehmen diskutiert. Wenngleich die Neuerungen von "Basel III" im Vergleich zur Vorgängerversion "Basel II" weniger für produzierende Unternehmen, denn für die Finanzbranche relevant ist, so wird doch deutlich, dass gerade viele kleine und mittlere Unternehmen, die "KMUs" in ihrem Management des Finanzwesen professioneller werden müssen. Eine Kreditvergabe an Unternehmen basiert heute, aufgrund der Vorschriften bei Banken und Sparkassen, unweigerlich auf einem Rating. Ein wesentlicher Bestandteil dieses Ratings ist die Fähigkeit von Unternehmer und Management, das Geschäftsrisiko zu erkennen und zu steuern. Ein situationsangepasstes und unternehmensgrößenadäquates Unternehmensrisiko-Management-System, oder, wie in der überwiegend englischsprachigen Literatur, Enterprise Risk Management System ("ERM") ist für den Ratingprozess unerlässlich, wenngleich auch nicht allein ausreichend. Ein weiterer Aspekt ist das Thema "Compliance" also das Befolgen rechtlicher Vorschriften und Rahmenbedingungen im umfassenden Sinn. Hier kann mangelndes Risikomanagement zu einer unmittelbaren Existenzbedrohung für Unternehmen, Unternehmer und Führungskräfte werden. Beispiele für hohe Bußgelder, strafrechtliche Verfolgung und Verurteilung von Personen und Ausschluss von Märkten bietet die Presse derzeit zu Hauf.

Mittlerweile bietet die Industrie hierzu auch ausgefeilte IT-gestützte Systeme an. Diese sind von Umfang und Funktionalität typischerweise extensiv angelegt und im Kontext großer Unternehmen und Konzerne die Lösung der Wahl. Für das typische KMU jedoch sind solche Systeme nicht nur in Anschaffung und Wartung, sondern auch im alltäglichen Handling zu umfangreich, zu teuer und zu (Personal-) ressourcenintensiv. Es gilt also, eine Lösung zu finden, welche die Ressourcen und Kapazitäten eines KMU nicht überstrapaziert:

1. Sie sollte einfach und schnell zu installieren sein,
2. sie sollte (Unternehmens-) umfassend und flexibel sein und
3. sie sollte als Basis für die Weiterentwicklung und eventuell spätere Installation eines IT gestützten Systems dienen können.

Im Folgenden versuchen wir ein solches System, das den oben genannten Anforderungen gerecht wird, zu skizzieren. Nachdem sich unser Ansatz in einigen Bereichen auf die angelsächsische Literatur stützt, haben wir die gängigen englischen Bezeichnungen in Klammern beigefügt.

Übersicht

Prinzipiell besteht ein ERM aus folgenden Komponenten:

1. einer Zuordnung von Verantwortlichkeiten in der Führung des Unternehmens sowie entsprechende Berichtsanforderungen zeitlicher und inhaltlicher Natur an die Geschäftsführung, bzw. Vorstand und Aufsichtsrat.
2. einer umfassenden Analyse der Risiken, ihres Schadenspotentials, Eintrittswahrscheinlichkeit und, gegebenenfalls, ihrer Interdependenz im Unternehmen sowie die Sammlung dieser in einer Datenbank (Risikoinventar oder Risk Inventory and Assessment "RIA").
3. einer Gruppe von Regeln, die den Umgang des Unternehmens mit seinen Risiken definiert. Diese sollte auf Ebene von Geschäftsführung, bzw. Vorstand und Aufsichtsrat mindestens
    a. die Risikopolitik der Gesellschaft im Kontext ihrer Risikotragfähigkeit ("Risikoappetit")

b. die Strategie im Umgang mit einzelnen Risiken (Akzeptieren, Vermindern, Vermeiden, Übertragen, Versichern)
c. Zuordnung der Risiko-Inhaberschaft, d. h. der individuellen Verantwortlichkeit für jedes spezifische Risiko.

Es versteht sich, dass das ERM bei Gruppen von Unternehmen jede Einheit umfassen soll und letztlich auf Konzernebene zusammen zu fassen ist.

Ein Fahrplan: Praktische Vorgehensweise zum Etablieren des ERM

Das Umsetzen erfolgt dann in einer Reihe von Schritten, jedoch muss sichergestellt werden, dass das ERM kein einmaliger Akt ist, sondern ein ständiger Begleiter in der Praxis der Unternehmensführung. Das ERM muss gelebt, regelmäßig überdacht und aktualisiert werden.

1. Schritt: Ordnen Sie die Verantwortlichkeit für das ERM. Benennen Sie den für das Risikomanagement verantwortlichen Geschäftsführer oder Vorstand, den Chief Risk Officer (CRO). Dies kann z. B. gleichzeitig auch der Finanzvorstand (CFO) oder Produktionsvorstand (COO) sein. Setzen Sie auch einen entsprechenden Stab für die tagtägliche Umsetzung und Dokumentation ein (dies müssen keine zusätzlichen Mitarbeiter sein, nur die Delegation auf entsprechende bestehende Mitarbeiter, z. B. den/die Assistent/-in des CRO, muss eindeutig sein).
2. Schritt: Um ein schnelles Resultat zu erzielen erstellen Sie das Risikoinventar (RIA) in einen Top-down Ansatz, d. h. durch die Geschäftsleitung/den Vorstand selbst, eventuell gemeinsam mit einem externen Berater. Dieses erste RIA muss in der Folge mit der Bottom-up Methodik erweitert, ergänzt, verfeinert, aktualisiert und ggf. korrigiert werden. Stellen Sie die Vollständigkeit des RIA sicher. Eine der zusätzlichen Kernfunktionen des Bottom-up Ansatzes ist, die Akzeptanz auf Ebene der Mitarbeiter und den zwischengelagerten Führungsebenen sicher zu stellen.
3. Schritt: Benennen Sie den Inhaber des Risikos ("Risk Owner"). Dies ist nicht zwangsläufig der CRO, sondern derjenige, der das Eingehen und die Steuerung eines Risikos faktisch in der Hand hat. Dies kann zum Beispiel in Fragen der Unternehmensstrategie der CEO sein, in IT-Fragen der Leiter der IT-Abteilung oder in Fragen der Kontrolle eines unberechtigten Zugangs zu den Geschäftsräumen der Leiter des Innendienstes. Diese Person ist für die Kontrolle des spezifischen Risikos, seines Berichtswesens und der Umsetzung der definierten Risikopolitik des Unternehmens verantwortlich. Simultan beschließen Sie in Kreis der Geschäftsleitung unter Mitwirkung des Risikoinhabers die Risikopolitik des Unternehmens: individuell für jedes Risiko, und aggregiert für Risikogruppen und letztlich das aggregierte Gesamtrisiko des Unternehmens. Dies schließt auch ein, zu bestimmen, welche Maßnahmen zu ergreifen sind, falls ein Risiko eintritt (Notfallpläne) und wie dies gegebenenfalls zu kommunizieren ist (Krisenkommunikation).
4. Schritt: Sammeln Sie die gesamte Dokumentation (von der Organisationsanweisung zum ERM über das RIA bis hin zu Notfallplänen und Kommunikationsrichtlinien) in einer Datenbank oder einem Handbuch (dem Risikohandbuch oder "Risk Manual"), zu der alle Mitarbeiter des Unternehmens Zugang haben. Stellen Sie sicher, dass alle Mitarbeiter, besonders aber Abteilungs- und Bereichsleiter mit dem Risikohandbuch vertraut sind.
5. Schritt: Bestimmen Sie einen festen Zeitplan und ein Schema für die Risikoberichterstattung und benennen Sie die (operativ) Verantwortlichen für die Berichterstattung. Der CFO wird diese Berichterstattung auf Unternehmensebene aggregieren. Halten Sie die Berichterstattung in den Protokollen der Geschäftsleitungssitzungen (gegebenenfalls auch in der Berichterstattung an den Aufsichtsrat) fest.
6. Schritt: Berufen Sie halbjährlich eine Arbeitssitzung zum ERM ein, vorzugsweise ein Treffen pro Jahr auf Geschäftsleiterebene und eines pro Jahr auf operativer Ebene, um das ERM fortzuentwickeln und zu verbessern. Diese Arbeitssitzungen können auch als Basis für die unter IFRS obligatorische Risikoberichterstattung dienen. Wobei in der Startphase die Arbeitssitzungen – zwecks Feinjustierung / Optimierung - kurzfristiger erfolgen müssen.

Wichtig ist zu verinnerlichen, dass das ERM gelebt und ständig fortentwickelt werden muss. Es ist an geänderte Unternehmensstrategien, geänderte Umweltbedingungen und geänderte Verhältnisse im Unternehmen selbst anzupassen. Sicher wird auch der Moment eintreten, da Unternehmensgröße und Komplexität ein per Hand geführtes ERM impraktikabel macht und ein IT-gestütztes System erfordert.

Schaubild: Beispiel für ein RIA Datenblatt

<table>
<tr><td colspan="2">Risikokategorie: [Anmerkung 1]</td><td colspan="2">Ggf. Risikosubkategorie</td></tr>
<tr><td colspan="4">Risikobeschreibung: [detaillierte Beschreibung des Risikos]</td></tr>
<tr><td colspan="2">Risikoinhaber: CEO/COO/CFO, Bereichsleiter [spezifizieren]</td><td colspan="2">Wichtigster Risikoindikator: [speziell Frühwarnsystem</td></tr>
<tr><td>Schadenshöhe: hoch/mittel/niedrig [Anmerkung 2]</td><td>Eintrittswahrscheinlichkeit: hoch/mittel/niedrig</td><td>Veränderung gegenüber Vorjahr: + / = / -</td><td>Priorität: hoch/mittel/niedrig</td></tr>
<tr><td colspan="2">Risikostrategie: Akzeptieren, Vermindern, Vermeiden, Übertragen, Versichern</td><td colspan="2">Überwachung: [Bestimmung der Personen und Instrumente, um das spezifische Risiko zu überwachen]</td></tr>
<tr><td colspan="4">Beschreibung der Risikostrategie: [detaillierte Beschreibung, mit welchen Maßnahmen und Instrumenten das Risiko gesteuert und die Risikopolitik des Unternehmens umgesetzt werden soll]</td></tr>
<tr><td colspan="4">Maßnahmen und Aktionen: [Handlungsanweisungen im Falle eines Eintritts des Risikos; auch: praktische Hinweise wie Notfallrufnummern etc.]</td></tr>
</table>

Anmerkung 1: Die Einteilung der Risiken erfolgt nach gängigen Schemata, z. B. strategische, operationelle, finanzielle und rechtliche Risiken, mit entsprechenden Subkategorien.

Anmerkung 2: In dem vereinfachten System wird auf eine betragsmäßige Bezifferung von Schadenshöhe, Eintrittswahrscheinlichkeit etc. verzichtet. Stattdessen schlagen wir ein Indikatorsystem vor, das zu Beginn sicher einfacher zu handhaben ist und auch (letztendlich irreführende) Scheingenauigkeit vermeidet. Auch hier sollte nach einer entsprechenden Erfahrung im Umgang mit dem ERM (hier insbesondere auch nach Gewinnen statistischer Werte) die Verfeinerung durch Anwendung quantitativer Verfahren angegangen werden.

Fazit:

Ein funktionierendes ERM ist bei den zunehmenden Anforderungen durch die Finanzwirtschaft ein zwingendes Muss für Unternehmen die sich in Wachstumsphasen oder aber auch in wirtschaftlich schwierigen Situationen mit Fremd- oder Eigenkapital besser positionieren wollen. Hierbei ist es unerheblich, ob eine gesetzliche Regelung für das Vorhandensein eines ERM besteht. Jeder Unternehmer und/oder Geschäftsführer sollte im eigenen Haftungsinteresse sich über die Risiken die sein Unternehmen bedrohen im Klaren sein. Hierzu zählen nicht nur unternehmerische Risiken sondern auch solche die aus Korruption und Wirtschaftskriminalität erwachsen können. Ein von allen Führungskräften und Mitarbeitern gelebtes System ist die beste Voraussetzung für eine effektive Unternehmensführung und -steuerung. Gleichzeitig bietet unser Ansatz ein ERM das zukunftsfähig ist und mit den wachsenden Anforderungen des Unternehmens weiterentwickelt werden kann, bis hin zur Migration auf ein IT-gestütztes System.

Dieser Artikel ist in der Online-Ausgabe der "Unternehmeredition" (ein Magazin der GoingPublic Media AG, München) erschienen.