Ein Bankenrechenzentrum macht die Pflicht zur Kür:

Risikomanagement als Unternehmenssteuerungswerkzeug

Frank Moritz/Uwe Kuhlmann

Viele Unternehmen überlegen derzeit, wie sie angemessen auf die veränderten gesetzlichen Rahmenbedingungen zum Risikomanagement reagieren können. Das Rechenzentrum eines großen Finanzdienstleisters hat sich entschlossen, das vom Wirtschaftsprüfer geforderte Risikomanagement-System nicht auf das gesetzlich notwendige Minimum zu beschränken, sondern als neues Werkzeug zur Unternehmenssteuerung auszubauen.

Hacker dringen in ein Rechenzentrum ein, ein Systemabsturz legt das Geschäft einer Bank lahm, die gesamte Concorde-Flotte muss für ein Jahr aus dem Verkehr gezogen werden, die Barings-Bank wird durch die kriminellen Machenschaften eines einzigen Mitarbeiters ruiniert: Die Medien berichten immer wieder über Ereignisse unterschiedlichster Art, die Unternehmen erheblich schädigen oder sogar vernichten können. Die Beispiele haben gemeinsam, dass diese Gefahren vorher vielen einzelnen Mitarbeitern bekannt waren, doch die Unternehmensleitung wusste nichts davon oder ignorierte das Problem einfach.

Risiken sind für ein Unternehmen jedoch immer Chance und Gefahr zugleich - wer keinerlei Risiko eingeht, macht auch kein Geschäft. Den richtigen Umgang mit bestehenden Risiken zu finden wird für Unternehmen zur wichtigen Zukunftsaufgabe.

Eine vorausschauende Risikopolitik kann Unternehmen vor vielen Risiken bewahren und auf den Notfall vorbereiten. Das schützt nicht nur das Unternehmen selbst, sondern auch seine Aktionäre, Mitarbeiter und Kunden. Auch der Gesetzgeber hat reagiert: Das 1998 verabschiedete "Gesetz zur Kontrolle und Transparenz in Unternehmen" (KonTraG) fordert, bestehende Risiken aufzuzeigen und der Unternehmensleitung sowie den Anteilseignern transparent zu machen. In eine ähnliche Richtung wird die "Eigenkapitalhinterlegungsrichtlinie Basel II" gehen, nach der Finanzdienstleister künftig die zu hinterlegenden Eigenmittel reduzieren können, wenn beispielsweise ein entsprechendes Risikomanagement nachgewiesen wird. Die genauen Inhalte dieser Richtlinie werden allerdings derzeit noch ausgehandelt.

Während früher vor allem Finanzrisiken im Visier des Risikomanagements standen, treten jetzt zunehmend die operativen Risiken in den Vordergrund, also diejenigen Risiken, die sich aus Geschäftsprozessen, Menschen, Systemen (und deren Zusammenspiel) oder externen Ereignissen ergeben. Dazu gehören beispielsweise fehlende Prozessbeschreibungen, "Wissensmonopole", das Einspielen nicht ausreichend getesteter IT-Systeme oder auch ein Seuchenalarm im benachbarten Krankenhaus. Vor diesem Hintergrund wurde bei dem Rechenzentrum, in dessen Verantwortung die gesamte IT-Produktion eines Finanzdienstleisters liegt, ein Risikomanagement eingeführt.

Einführung des Risikomanagements

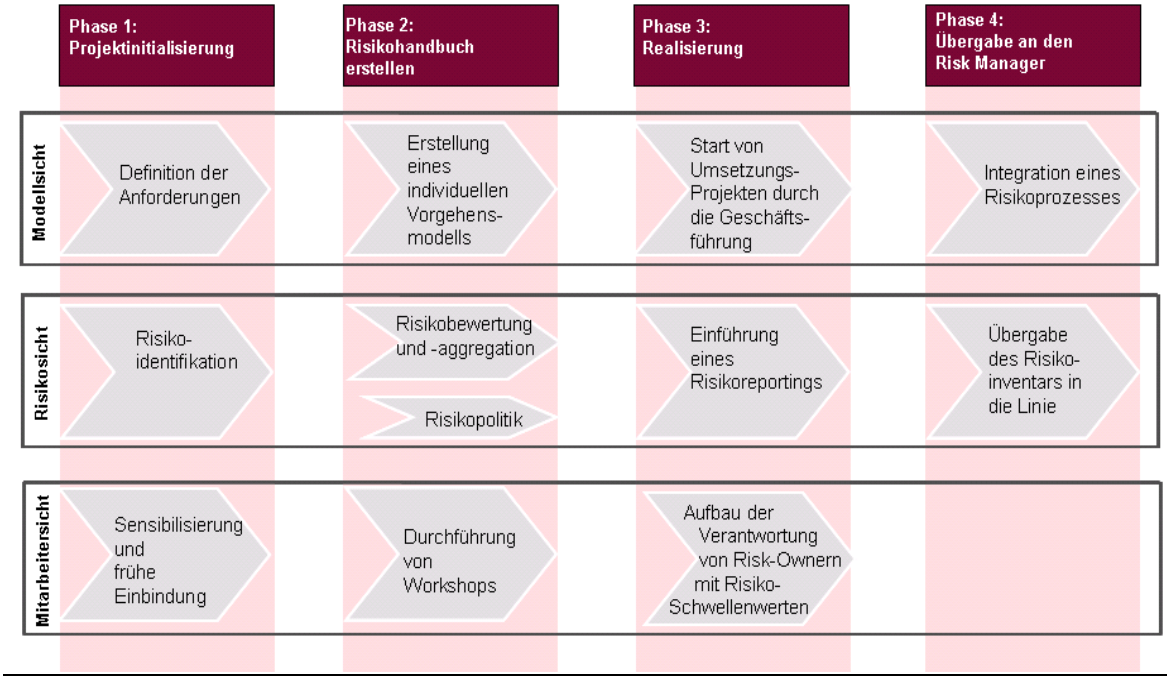
Ein Unternehmen, das Risikomanagement einführen möchte, muss sich zu Beginn mit der Frage auseinander setzen, welche Ziele es damit verfolgen will. Sollen nur die gesetzlichen Mindestanforderungen erfüllt werden? Damit würde man aber wichtige Ergebnisse des Projektes praktisch ungenutzt verschenken. Das Rechenzentrum entschied sich dafür, die einmal erhobenen Daten zu einem umfassenden Unternehmenssteuerungswerkzeug auszubauen, das verschiedenartige Probleme des Unternehmens an der Basis erfasst, strukturiert, bewertet und die Risikominimierung steuert.

Die Einführung eines Risikomanagements ist ein einmaliges, individuell an das Unternehmen anzupassendes Projekt mit unternehmensweitem Charakter. Daher sollten folgende Rahmenbedingungen erfüllt sein:

- Die Beauftragung muss direkt durch die Geschäftsführung erfolgen.
- Auch die Berichtspflicht richtet sich direkt an die Geschäftsführung.
- Die Risikopolitik des Unternehmens sollte in einer frühen Projektphase formuliert werden.
- Es gibt einen Projektleiter für die Einführung. Er muss nicht unbedingt mit dem späteren Risikomanager identisch sein, der im Anschluss an das Projekt die Aufgaben in der Linie übernimmt.
- Der künftige Risikomanager sollte so früh wie möglich in das Projekt eingebunden sein.
- Für die Einführung des Risikomanagements wird ein Budget veranschlagt. Weiterhin müssen schwerwiegende Risiken, die im Laufe des Projektes erkannt werden, sofort durch vorgezogene Umsetzungsprojekte behandelt werden.
- Die Projektleiter der gestarteten Umsetzungsprojekte sollten dem Gesamtprojektleiter "Einführung Risikomanagement" gegenüber berichtspflichtig sein. Dieser wiederum unterstützt die Teilprojektleiter bei der Durchführung.

Im konkreten Projekt hat sich darüber hinaus ein Vorgehen in vier Phasen bewährt (Abb. 1)

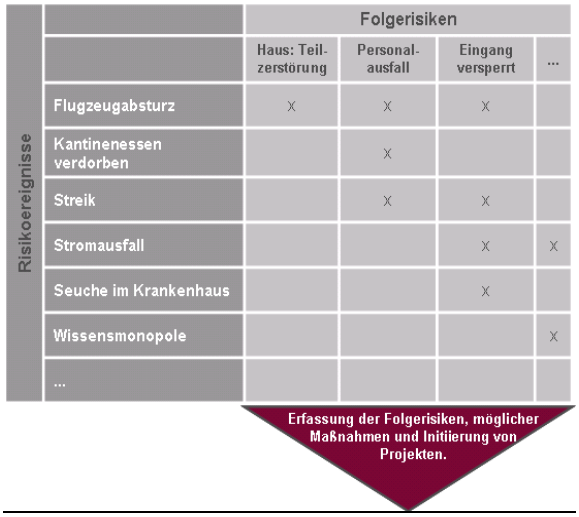
Abb. 1: Phasenmodell der Einführung



Die Informationsflut beherrschen

Bei der ersten Risikoerhebung im Rechenzentrum wurde unterschieden zwischen abteilungs- und teaminternen Risiken, abteilungs- und teamübergreifenden Risiken, Schnittstellenrisiken (EDV, Geschäftsprozesse) und Managementrisiken. Je nach Zielsetzung wurden diese Informationen in moderierten Workshops nur mit Führungskräften oder mit den Mitarbeitern an der Basis erhoben und diskutiert. Dadurch wurde gleichzeitig eine Sensibilisierung für das Thema und eine Identifikation mit dem Projekt erreicht. Anschließend wurden die Risiken bewertet und zusammengeführt. Überraschend und positiv für das Projekt war die große Akzeptanz und Mitarbeit in allen Unternehmensbereichen. Die Mitarbeiter erkannten das Risikomanagement als Eskalationsinstanz für noch nicht behandelte Risiken an. Das Problem: Theoretisch gibt es eine unübersehbare Vielfalt möglicher Risiken und denkbarer Auswirkungen. Auch die Mitarbeiter und Führungskräfte des Rechenzentrums führten zu Beginn des Projekts eine Vielzahl scheinbar unlösbarer Risiken auf, die zunächst einmal kanalisiert und auf irgendeine Weise handhabbar gemacht werden mussten. Die gängige Literatur zum Thema bietet dafür leider noch keine griffigen Lösungen. Im geschilderten Projekt hat es sich bewährt, bei der Risikoklassifizierung zwischen Risikoereignissen und Folgerisiken unterschieden. Risikoereignisse sind demnach mögliche Risiken für das Unternehmen, die im weiteren Verlauf Folgerisiken mit negativen Auswirkungen auf die Wertschöpfungskette nach sich ziehen können (Abb. 2): Das Risikoereignis "Flugzeugabsturz in der Nähe des Unternehmens" etwa kann zu einer teilweisen Zerstörung des Gebäudes führen; als Folgerisiken wären beispielsweise Personalausfälle oder der Ausfall eines oder mehrerer IT-Systeme denkbar. Umgekehrt könnte das Folgerisiko "Ausfall eines oder mehrerer IT-Systeme" durch den genannten Flugzeugabsturz, aber auch durch einen Hackerangriff oder einen Stromausfall ausgelöst werden.

Abb. 2: Risiken und Folgerisiken

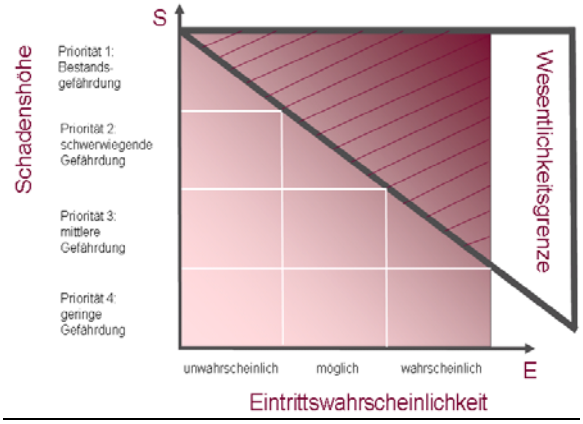


Der entscheidende Vorteil dieser Klassifizierung: Es ist nicht wesentlich, welches Risikoereignis ein Folgerisiko hervorruft, denn die erforderlichen Notfallmaßnahmen sind oft die gleichen. Es mussten also nicht sämtliche möglichen Risikoereignisse, sondern nur die denkbaren Folgerisiken betrachtet werden. Dadurch ließ sich die Anzahl der zu behandelnden Risiken erheblich reduzieren. Alle bewerteten Risiken wurden in einem Risikohandbuch zusammengeführt, das auch zur Initiierung erster Umsetzungsprojekte (z. B. Entwicklung von Notfallplänen, Qualifizierungspläne für Mitarbeiter) genutzt wurde. Dazu war natürlich zunächst eine Priorisierung erforderlich, zu der zwischen wesentlichen Risiken - aktuell und bestandsgefährdend - und weniger wesentlichen Risiken unterschieden wurde (Abb. 3). Für alle Risiken wurden jeweils verantwortliche "Risk-Owner" definiert, die die Risiken entsprechend bewerten mussten und in Zukunft weiter beobachten müssen.

Die Aufgaben des Risk-Managers

Mit dem Aufbau eines Risikohandbuchs ist allerdings nur der erste Schritt getan. Risiken verändern sich im Laufe der Zeit, neue Risiken kommen hinzu, bekannte treten in den Hintergrund. Aus der Risikobetrachtung muss also ein ständiger Prozess werden. Dazu wurde bei dem Rechenzentrum ein Risk-Manager eingesetzt, der die Berichte der Risk-Owner zusammenführt und diese bei der Risikobewältigung unterstützt. Er berichtet direkt an die Unternehmensleitung.

Abb. 3: Wesentlichkeitsgrenze für erhobene Risiken



Je nach Risikopolitik eines Unternehmens übernimmt ein Risk-Manager unterschiedliche Aufgaben. Beschränkt sich die Risikopolitik auf die Erfüllung der gesetzlichen Anforderungen, so fungiert der Risk-Manager vor allem als Ansprechpartner der Unternehmensleitung, Multiprojektleiter und Lenker der Risk-Owner. Soll das Risikomanagement gleichzeitig als Unternehmenssteuerungswerkzeug dienen, so übernimmt der Risk-Manager zusätzliche Aufgaben in der aktiven Risikosteuerung, der Mitarbeitermotivation etc. Eine solche Stabsstelle sollte, je nach Ausprägung, als eigener Bereich oder im Quality-Management eingerichtet werden.

Aus Sicht des Rechenzentrums hat es sich gelohnt, das Risikomanagement über die gesetzlichen Anforderungen hinaus zu einem Unternehmenssteuerungswerkzeug weiterzuentwickeln. Nach einer umfassenden Betrachtung aller Risikofelder der Organisation, über sämtliche Querschnittsfunktionen und Prozesse hinweg, ist der Einstieg in eine kontinuierliche Risikobetrachtung des Unternehmens gelungen: Dank der an verschiedenen Stellen verankerten Verantwortung und der erreichten Sensibilisierung dürften neu aufkommende Risiken schnell als solche identifiziert werden und geeignete Gegenmaßnahmen zeitnah eingeleitet werden.

Autoren:

Frank Moritz ist leitender Berater bei der Ropardo AG, Leverkusen.

Uwe Kuhlmann ist Senior-Berater im Geschäftsführungsstab Sonderprojekte beim Rechenzentrum eines Finanzdienstleisters in Düsseldorf.