Erfolgreiches Risikomanagement mit COSO ERM

Empfehlungen für die Gestaltung und Umsetzung in der Praxis

Von

Christian Brünger

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über
dnb.ddb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 11439 9

ISBN 978 3 503 11439 9

Dieses Papier erfüllt die Frankfurter Forderungen
der Deutschen Nationalbibliothek und der Gesellschaft
für das Buch bezüglich der Alterungsbeständigkeit und
entspricht sowohl den strengen Bestimmungen der US Norm
Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Druck und Bindung: Hubert & Co., Göttingen

Vorwort

Leute, die sich die Finger verbrennen, verstehen nichts vom Spiel mit dem Feuer.

Oscar Wilde

Spätestens seit dem Jahre 1998 zählt das Risikomanagement durch das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich* (KonTraG) zu den festen Unternehmensbestandteilen. Jedoch spricht der Gesetzestext nicht wörtlich von einem Risikomanagementsystem, sondern lediglich von einem Überwachungssystem, das *bestandsgefährdende Entwicklungen* frühzeitig erkennt. Erst zehn Jahre später wird der Begriff „Risikomanagement" durch das *Bilanzrechtsmodernisierungsgesetz* (BilMoG) wörtlich in den Gesetzestext aufgenommen. Mit dem BilMoG wird die gesetzliche Forderung nach einem Risikomanagementsystem im Unternehmen weiter verstärkt.

Die verbreitete Sichtweise, Risikomanagement diene lediglich dazu, gesetzliche Anforderungen zu erfüllen, ist nicht angemessen. Auch wenn die gesetzlichen Vorschriften sich nicht auf alle Unternehmen beziehen, sollte dennoch jedes Unternehmen ein Risikomanagement in der einen oder anderen Form betreiben, um die Unternehmensrisiken zu beherrschen.

Jede korrekt durchgeführte Kontrolle hätte mein System aufgedeckt.

Jérôme Kerviel nach seiner Festnahme im Jahre 2008. Kurz zuvor verlor die Société Générale ca. 4,9 Mrd. EUR durch seine Handlungen.

Insbesondere in vielen mittelständischen, aber auch in manchen großen Unternehmen wird Risikomanagement lediglich als gesetzliche Pflichterfüllung betrachtet. Der Nutzen wird dabei nicht erkannt, sodass häufig das Ziel verfolgt wird, die regulatorischen Anforderungen an das Risikomanagement mit minimalem Aufwand zu erfüllen. Ein solcher Ansatz führt dazu, dass Risikomanagement zu einem reinen Kostenfaktor wird. Der Nutzen, der sich unter anderem durch die bewusste Steuerung von Risiken und die Ausbildung eines Risikobewusstseins ergibt, kann die Kosten aber deutlich übersteigen und ist mit dem Ziel der absoluten Kostenminimierung im Risikomanagement nicht vereinbar. Wie überall gibt es auch im Risikomanagement keinen „*free lunch*"; Risikomanagement kostet – gutes Risikomanagement bringt mehr als es kostet – schlechtes oder gar kein Risikomanagement kostet häufig die Unternehmensexistenz.

Doch wie gestaltet man ein gutes Risikomanagementsystem im Unternehmen? Gibt es einen „Königsweg“, der für jedes Unternehmen gilt? Grundsätzlich muss jedes Unternehmen seinen eigenen Weg finden. Jedoch ist eine Orientierung an bisherigen Erkenntnissen und Erfahrungen anderer ein durchaus gewinnbringender Ansatz im Vergleich zu einer Risikomanagemententwicklung im Freistil.

Auch wenn das Thema Risikomanagement bereits seit einiger Zeit in Wirtschaft und Wissenschaft diskutiert wird, haben sich erst wenige aktuelle international anerkannte Rahmenmodelle für ein unternehmensweites Risikomanagement entwickelt. Zu den umfassenderen Werken zählen der Australisch/Neuseeländische Standard AS/NZS 4360, der Österreichische Standard ON49000ff. und das amerikanische Rahmenmodell COSO ERM. Daneben existieren noch einige weniger umfassende Werke wie der Risikomanagementstandard der FERMA. Die ISO-Organisation erarbeitet zurzeit eine weltweite Risikomanagementnorm ISO 31000. Die Entwürfe zeigen jedoch, dass diese Norm keine wesentliche Neuerung darstellt. Zudem wird die ISO-Norm auch keine zertifizierbare Norm werden. Eine Zertifizierung des Risikomanagements, wie es sie für das Qualitätsmanagement gibt, ist daher nicht zu erwarten. Neben den Rahmenmodellen für das unternehmensweite Risikomanagement existiert jedoch noch eine schier unüberschaubare Anzahl an Vorgehensweisen und Rahmenmodellen für spezielle Bereiche oder Branchen, die nur bedingt für die Konzeption eines unternehmens- und branchenübergreifenden Systems geeignet sind.

Das COSO-ERM-Rahmenmodell ist eines der international anerkannten Rahmenmodelle im Risikomanagement. Durch seine Entwicklungshistorie ist es eines der Referenzmodelle für Wirtschaftsprüfer. Zudem beantwortet dieses Modell auch die Frage nach den Gemeinsamkeiten, Unterschieden und Berührungspunkten zwischen einem unternehmensweiten Risikomanagementsystem und einem internen Kontrollsystem. Dadurch wird eine effiziente Umsetzung des Risikomanagements ermöglicht. Nicht zuletzt ist das COSO ERM auch sehr flexibel in seiner Ausgestaltung, sodass es für Unternehmen jeder Größe und insbesondere auch für den Mittelstand geeignet ist.

Das vorliegende Buch fokussiert auf das Rahmenmodell *COSO Enterprise Risk Management*. Dennoch ist es keine Übersetzung des englischsprachigen COSO-ERM-Rahmenmodells. Vielmehr erfolgt eine zusammenfassende, überblicksartige Darstellung dieses Rahmenmodells, die um praktische Methoden, Umsetzungshilfen und Praxisbeispiele ergänzt wird. Das Buch richtet sich an Praktiker, die ein unternehmensweites Risikomanagementsystem neu konzipieren und umsetzen möchten. Aber auch wenn bereits ein Risikomanagementsystem in einem Unternehmen vorhanden ist, kann mit dem vorliegenden Buch ein Abgleich erfolgen und somit Optimierungspotenzial aufgedeckt werden. Insbesondere ist das Buch auch für Leser interessant, die bisher nur Einblicke in einen Teilbereich des Risikomanagements gewinnen konnten und nun einen Überblick über das unternehmensweite Risikomanagement als Ganzes erlangen möchten. Auch wissenschaftlich orientierte Leser erhalten einen Eindruck von den Methoden, die Praktiker einsetzen, um

Probleme in der Praxis zu lösen. Nicht zuletzt ist das Buch für alle diejenigen geeignet, die sich in das Thema Risikomanagement einarbeiten wollen. Die Inhalte wurden bewusst so strukturiert und formuliert, dass auch Leser mit nur geringem Vorwissen ein Verständnis für das unternehmensweite Risikomanagement nach COSO ERM erlangen können.

Ein Dank gilt all denjenigen, die dieses Werk unterstützt und gefördert haben. Ohne die folgenden Personen, wäre das vorliegende Buch nicht in dieser Form entstanden. Ihnen gilt daher (in alphabetischer Reihenfolge) ein ganz besonderer Dank: Stephan Beeusaert, Reimund Bohm, Claudia Brandt, Bernd-Uwe Frank, Nina Lissen, Prof. Dr. Betina Schiller, Wilhelm F. Stute und Prof. Dr. Franz Wagner.

Paderborn im Juni 2009 Christian Brünger

Inhaltsverzeichnis