Unternehmensweites Risikomanagement - Übergreifendes Rahmenwerk

Zusammenfassung

The Committee of Sponsoring Organizations
of the Treadway Commission

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight	Representative
COSO Chair	John J. Flaherty
American Accounting Association	Larry E. Rittenberg
American Institute of Certified Public Accountants	Alan W. Anderson
Financial Executives International	John P. Jessup Nicholas S. Cyprus
Institute of Management Accountants	Frank C. Minter Dennis L. Neider
The Institute of Internal Auditors	William G. Bishop, III David A. Richards

Project Advisory Council to COSO

Guidance

Tony Maki, Chair	James W. DeLoach	John P. Jessup
Partner *Moss Adams LLP*	*Managing Director* *Protiviti Inc.*	*Vice President and Treasurer* *E. I. duPont de Nemours and Company*
Mark S. Beasley	Andrew J. Jackson	Tony M. Knapp
Professor *North Carolina State University*	*Senior Vice President of Enterprise Risk Assurance Services* *American Express Company*	*Senior Vice President and Controller* *Motorola, Inc.*
Jerry W. DeFoor	Steven E. Jameson	Douglas F. Prawitt
Vice President and Controller *Protective Life Corporation*	*Executive Vice President, Chief Internal Audit & Risk Officer* *Community Trust Bancorp, Inc.*	*Professor* *Brigham Young University*

PricewaterhouseCoopers LLP

Author

Principal Contributors

Richard M. Steinberg	Miles E.A. Everson
Former Partner and Corporate Governance Leader (Presently Steinberg Governance Advisors)	*Partner and Financial Services Finance, Operations, Risk and Compliance Leader* *New York*
Frank J. Martens	Lucy E. Nottingham
Senior Manager, Client Services *Vancouver, Canada*	*Manager, Internal Firm Services* *Boston*

Vorwort

Vor mehr als einem Jahrzehnt veröffentlichte das Committee of Sponsoring Organizations of the Treadway Commission (COSO) das Rahmenwerk „*Interne Kontrolle - Übergreifendes Rahmenwerk“* mit dem Ziel, Unternehmen und andere Organisationen in der Bewertung und der Verbesserung ihrer Internen Kontrollsysteme zu unterstützen. Jenes Rahmenwerk wurde seitdem in Vorschriften, Regeln und Verordnungen umgesetzt. Tausende von Unternehmen nutzen es bereits, um alle Aktivitäten auf das Erreichen festgelegter Ziele auszurichten.

In den letzten Jahren hat sich ein stärkeres Interesse in Bezug auf die Ausrichtung des Risikomanagements entwickelt. Es wurde zunehmend klar, dass erheblicher Bedarf an einem schlüssigen Rahmenwerk zur wirksamen Bestimmung, Bewertung und Steuerung von Risiken besteht. Im Jahr 2001 hat COSO ein Projekt ins Leben gerufen und PricewaterhouseCoopers beauftragt, ein Rahmenwerk zu entwickeln, das von Führungskräften direkt anwendbar ist. Das unternehmensweite Risikomanagement einer Organisation soll damit bewertet und verbessert werden können.

Während der Entwicklung des Modells kam es zu einer Serie schwerer Wirtschaftsskandale und Unternehmenszusammenbrüche, bei denen Investoren, Mitarbeiter und andere Interessengruppen erhebliche Verluste erlitten. Die Folge hierauf waren Forderungen nach verbesserter Unternehmensführung und einem verbesserten Risikomanagement sowie neue Gesetze, Verordnungen und Vorschriften für börsennotierte Unternehmen. Der Bedarf an einem Rahmenwerk zu einem unternehmensweiten Risikomanagement, das Kernprinzipien und -konzepte, eine einheitliche Terminologie sowie klare Anweisungen und Hilfestellungen bereitstellt, wurde dadurch nochmals unterstrichen. COSO ist der Ansicht, dass das Rahmenwerk „*Unternehmensweites Risikomanagement - Übergreifendes Rahmenwerk“* diese Ziele erreicht, und erwartet deshalb, dass es weite Verbreitung in Unternehmen, in anderen Organisationen sowie Interessengruppen finden wird.

In Folgen der eben dargestellten Problematik wurden in den USA der Sarbanes Oxley Act 2002 sowie ähnliche Gesetzgebungsvorhaben in anderen Ländern ergriffen. Das US-amerikanische Gesetz ergänzt, durch die Forderung Interne Kontrollsysteme zu installieren, die schon länger bestehenden Regelungen für börsennotierte Gesellschaften. Hiebei müssen Führungskräfte die Funktionsfähigkeit dieser Systeme bestätigen und von Abschlussprüfern testieren lassen. Das Rahmenwerk „*Interne Kontrolle - Übergreifendes Rahmenwerk“* bildet auch weiterhin die akzeptierte Grundlage, um den Anforderungen gerecht zu werden.

Die Veröffentlichung „*Unternehmensweites Risikomanagement - Übergreifendes Rahmenwerk“* stellt eine Ergänzung dar, indem es in stärkerem Maße den Schwerpunkt im Bereich des allgemeinen, unternehmensweiten Risikomanagements setzt. Da es nicht als Ersatz des Internen Kontrollmodells vorgesehen und geeignet ist, sondern auf diesem aufbaut, können Unternehmen das vorliegende unternehmensweite Risikomanagementmodell nutzen, um ihre Internen Kontrollsysteme zu gestalten und hin zu einem umfassenderen Risikomanagementsystem zu entwickeln.

Eine der größten Herausforderungen für Führungskräfte ist es zu bestimmen, in welchem Umfang eine Organisation bereit und willens ist, im Zuge des Wertschöpfungsprozesses Risiken auf sich zu nehmen. Dieses Dokument soll Sie unterstützen, dieser Herausforderung besser zu begegnen.

John J. Flaherty
Vorsitzender, COSO

Tony Maki
Vorsitzender, COSO Advisory Council

Zusammenfassung

Die grundlegende Annahme des unternehmensweiten Risikomanagements ist, dass jede Organisation für spezifische Interessengruppen Werte schafft. Alle Organisationen sind hierbei Unsicherheiten ausgesetzt. Die Aufgabe der Führungskräfte ist daher zu bestimmen, wie viel Unsicherheit sie, bei dem Versuch Werte für die Interessengruppen zu schaffen, akzeptieren. Unsicherheit umfasst sowohl Risiken als auch Chancen und die Möglichkeit, Werte zu vernichten oder zu vermehren. Das unternehmensweite Risikomanagement ermöglicht daher Führungskräften wirksam mit Unsicherheit und den damit einhergehenden Risiken und Chancen umzugehen und hierbei ihre Fähigkeit zur Wertschöpfung zu stärken.

Werte sind maximiert, wenn die Führungskräfte Strategien und Ziele festlegen, die ein optimales Gleichgewicht zwischen Wachstums- und Ertragszielen sowie den damit einhergehenden Risiken ermöglichen. Ein wirtschaftlicher und wirksamer Einsatz von Ressourcen bei der Umsetzung der Organisationsziele soll erzielt werden. Unternehmensweites Risikomanagement umfasst:

- *Anpassung von Risikoneigung und Strategie* – Die Führungskräfte berücksichtigen die Risikoneigung der Organisation bei der Beurteilung strategischer Alternativen, dem Setzen entsprechender Ziele, und bei der Entwicklung von Mechanismen zur Steuerung der damit einhergehenden Risiken.
- *Verbessern von risikobezogenen Entscheidungen* – Das Unternehmensweite Risikomanagement stellt ein Vorgehen zur Bestimmung und Auswahl von alternativen Reaktionen auf Risiken zur Verfügung – Risikovermeidung, Risikoverringerung, Risikoverteilung und Risikoübernahme.
- *Verringern von Überraschungen und Verlusten im Geschäftsbetrieb* - Organisationen verbessern ihre Fähigkeit, mögliche Ereignisse zu erkennen und Maßnahmen einzuleiten sowie Überraschungen und die damit einhergehenden Kosten oder Verluste zu verringern.
- *Bestimmen und Steuern mehrfacher und unternehmensübergreifender Risiken* – Jedes Unternehmen steht einer Vielzahl von Risiken gegenüber, die mehrere Unternehmensbereiche betreffen. Zudem ermöglicht das unternehmensweite Risikomanagement wirksame Reaktionen auf die voneinander abhängigen Wirkungen sowie auf übergreifende Maßnahmen bei Mehrfachrisiken.
- *Nutzen von Chancen* – Das Berücksichtigen aller möglichen Ereignisse ermöglicht Führungskräfte, Chancen zu erkennen und proaktive umzusetzen.
- *Verbesserte Kapitalallokation* – Zuverlässige Risikoinformationen erlauben Führungskräfte, die Kapitalausstattung gesamthaft zu beurteilen und die Kapitalzuordnung zu verbessern.

Diese im unternehmensweiten Risikomanagement enthaltenen Fähigkeiten unterstützen Führungskräfte dabei, die Ergebnis- und Ertragsziele ihrer Organisation zu erreichen und den Verlust von Ressourcen zu verhindern. Das Unternehmensweite Risikomanagement hilft bei der Sicherstellung funktionsfähiger Berichtssysteme sowie beim Einhalten von Gesetzen und Vorschriften. Darüber hinaus trägt es dazu bei, die Beschädigung des Rufs der Organisation sowie die damit einhergehenden Folgen zu vermeiden. Zusammenfassend kann formuliert werden: Das Risikomanagement unterstützt eine Organisation, die gesetzten Ziele zu erreichen und Störungen sowie Überraschungen zu vermeiden.

Ereignisse - Risiken und Chancen

Ereignisse können negative oder positive Auswirkungen haben. Ereignisse mit negativen Auswirkungen bedeuten Risiken, die Wertschöpfung verhindern oder bestehende Werte reduzieren können. Ereignisse mit positiven Auswirkungen hingegen können negative Effekte ausgleichen oder Chancen eröffnen. Chancen sind somit Ereignisse, die dass Erreichen von Zielen fördern und zur Wertschöpfung bzw. -erhaltung beitragen. Führungskräfte nutzen Chancen im Zuge ihres Strategie- bzw. Zielsetzungsprozesses, indem sie die das Nutzen der Chancen systematisch planen.

Unternehmensweites Risikomanagement definiert

Das Unternehmensweite Risikomanagement betrifft Risiken und Chancen, die die Wertschöpfung beeinflussen. Der Terminus Risikomanagement ist wie folgt definiert:

> *Unternehmensweites Risikomanagement ist ein Prozess, ausgeführt durch Überwachungs- und Leitungsorgane, Führungskräfte und Mitarbeiter einer Organisation, angewandt bei der Strategiefestlegung sowie innerhalb der Gesamtorganisation, gestaltet um die die Organisation beeinflussenden, möglichen Ereignisse zu erkennen, und um hinreichende Sicherheit bezüglich des Erreichens der Ziele der Organisation zu gewährleisten.*

Die Definition berücksichtigt einige grundlegende Konzepte. Das Unternehmensweite Risikomanagement ist/ wird:

- ein Prozess, der sich ununterbrochen und über die gesamte Organisation erstreckt
- ausgeführt durch Menschen auf jeder Ebene einer Organisation
- angewandt bei der Strategiefestlegung
- unternehmensübergreifend angewandt – auf jeder Ebene und in jeder Einheit – und betrachtet das organisationsweite Risikoportfolio
- gestaltet, um mögliche Ereignisse zu erkennen – die im Falle ihres Eintretens die Organisation beeinflussen – und um Risiken auf Grundlage der Risikoneigung zu steuern
- Geeignet, den Führungskräften sowie dem Überwachungs- und Leitungsorganen einer Organisation hinreichend Sicherheit zu gewährleisten
- Ausgerichtet auf das Erreichen von Zielen in einer oder mehreren zusammenhängenden Kategorien

Diese Definition ist absichtlich breit gewählt. Sie deckt grundlegende Konzepte ab, die eine Basis dafür bilden, wie Unternehmen und andere Organisationen Risiken steuern. Gleichzeitig bietet sie so eine Grundlage für die organisations-, unternehmens- und branchenübergreifende Anwendung. Sie ist direkt auf das Erreichen von Zielen ausgerichtet, die von einer Organisation festgelegt sind und bildet eine Grundlage für die Beurteilung der Funktionsfähigkeit des unternehmensweiten Risikomanagements.

Erreichen von Zielen

Im Rahmen der für eine Organisation festgelegten Mission oder Vision setzen Führungskräfte strategische Ziele fest, wählen die Strategie aus und brechen Ziele auf die Ebenen der Organisation herunter. Dieses Rahmenwerk für unternehmensweites Risikomanagement ist darauf ausgerichtet, die Ziele einer Organisation zu erreichen, welche sich in i.d.R. in vier Kategorien gliedern:

- *Strategische* Ziele – übergeordnete Ziele, die mit der Mission abgestimmt sind und diese unterstützen
- *Betriebliche Ziele* – wirksamer und wirtschaftlicher Ressourceneinsatz
- *Berichterstattung* – Zuverlässigkeit der Berichterstattung
- *Regeleinhaltung* – Einhalten anwendbarer Gesetze und Vorschriften

Die Kategorisierung von Organisationszielen ermöglicht eine Ausrichtung auf verschiedene Aspekte des unternehmensweiten Risikomanagements. Die unterscheidbaren, aber überlappenden Kategorien – ein spezifisches Ziel kann in mehr als eine Kategorie fallen – berücksichtigen verschiedene organisationsbedingte Bedürfnisse und können in die direkte Verantwortung unterschiedlicher Führungskräfte fallen. Die Kategorisierung erlaubt zudem die Unterscheidung der Erwartungen an die jeweiligen Zielkategorien. Eine weitere von einigen Organisationen genutzte Kategorie, die Sicherung des betrieblichen Vermögens, wird ebenfalls beschrieben.

Da die Ziele in Bezug auf die Zuverlässigkeit der Berichterstattung sowie das Einhalten von Gesetzen und Vorschriften der Kontrolle einer Organisation unterliegen, kann das unternehmensweite Risikomanagement hinreichend Sicherheit bezüglich des Erreichens dieser Ziele gewährleisten. Das Erreichen strategischer und betrieblicher Ziele wird aber auch beeinflusst durch externe Ereignisse, die sich nicht immer durch die Organisation kontrollieren lassen. Daher kann das unternehmensweite Risikomanagement bezüglich dieser Ziele hinreichend Sicherheit geben, dass Führungskräfte im Rahmen ihrer Überwachungsfunktion sowie Überwachungs- und Leitungsorgane zeitnah darüber Kenntnis erhalten, in welchem Maß sich die Organisation dem Erreichen der Ziele nähert.

Komponenten des unternehmensweiten Risikomanagements

Das unternehmensweite Risikomanagement besteht aus acht wechselseitig verknüpften Komponenten. Diese leiten sich daraus ab, wie Führungskräfte ein Unternehmen steuern und sich mit dem Führungsprozess verknüpft. Die Komponenten sind:

- *Internes Umfeld* - Das interne Umfeld beschreibt die Kultur einer Unternehmung und bildet die Grundlage dafür, wie Risiken durch die Mitarbeiter der Organisation betrachtet und behandelt werden – hierbei miteingeschlossen sind die Risikophilosophie und -bereitschaft, Integrität und ethische Werte. Zudem beschreibt das Interne Umfeld die Gegebenheiten, in dem das Unternehmen agiert.

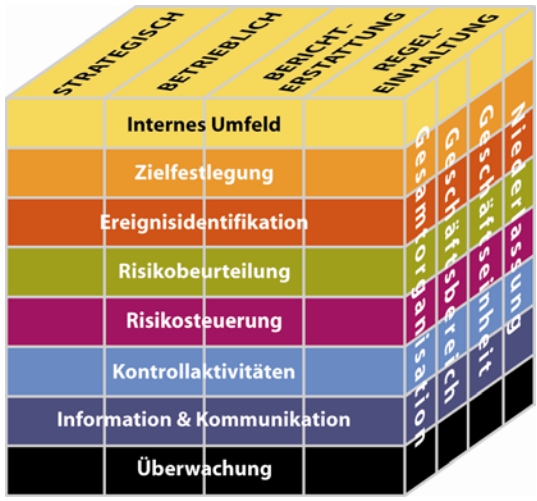
- *Zielfestlegung* - Ziele müssen festgelegt sein, bevor Führungskräfte mögliche Ereignisse, die deren Erreichen beeinflussen, bestimmen können. Das Unternehmensweite Risikomanagement ist Teil eines Prozesses um Ziele zu setzen und um sicher zu stellen, dass die gewählten Ziele die Mission einer Organisation unterstützen, damit übereinstimmen und der Risikoneigung gerecht werden.
- *Ereignisidentifikation* - Interne und externe Ereignisse, die das Erreichen der Ziele einer Organisation beeinflussen, müssen bestimmt und in Risiken und Chancen unterschieden werden. Chancen gehen in den Strategiebildungs- oder Zielsetzungsprozess der Führungskräfte ein.
- *Risikobeurteilung* - Risiken werden unter Berücksichtigung von Auswirkung und Eintrittswahrscheinlichkeit untersucht, um eine Grundlage für ihre Steuerung zu erhalten. Sowohl innewohnende Risiken als auch Restrisiken sollen bewertet werden.
- *Risikosteuerung* - Führungskräfte wählen Instrumente zur Risikosteuerung - Vermeiden, Annehmen, Verringern oder Teilen von Risiko - um ein Bündel von Maßnahmen zum Anpassen der Risiken an die Risikotoleranz und -bereitschaft der Organisation festzulegen.
- *Kontrollaktivitäten* - Vorschriften und Verfahren, die sicherstellen, dass Risikoreaktionen wirksam ausgeführt werden, werden festgelegt und umgesetzt.
- *Information und Kommunikation* - Wesentliche Informationen sind in Form und Zeitrahmen erkannt, erfasst und verbreitet. Diese ermöglichen es Mitarbeitern, ihre Verantwortlichkeit wahrzunehmen. Wirksame Kommunikation findet auch in einem weiteren Sinne statt, abwärts, lateral und aufwärts in der Organisation.
- *Überwachung* - Die Gesamtheit des unternehmensweiten Risikomanagements wird überwacht und erforderliche Anpassungen werden vorgenommen. Überwachung wird durch laufende Führungstätigkeiten und separate Beurteilungen erreicht.

Unternehmensweites Risikomanagement ist kein streng linearer Ablauf, bei dem eine Komponente nur die angrenzende Komponente beeinflusst. Es ist ein multidirektionaler, iterativer Ablauf, bei dem nahezu jede Komponente jede andere Komponente beeinflussen kann und wird.

Beziehung zwischen Zielen und Komponenten

Es gibt eine direkte Beziehung zwischen Zielen, die wiedergeben, was eine Organisation erreichen will, und Komponenten des unternehmensweiten Risikomanagements, die wiedergeben, was zu ihrem Erreichen erforderlich ist. Diese Beziehungen werden in einem dreidimensionalen Modell in Form eines Würfels dargestellt.

Die vier Zielkategorien - strategisch, betrieblich, Berichterstattung und Regeleinhaltung - sind in den vertikalen Spalten dargestellt, die acht Komponenten durch horizontale Reihen, und die Einheiten einer Organisation durch die dritte Dimension. Diese Darstellung gibt die Möglichkeit wieder, sich entweder auf die Gesamtheit des unternehmensweiten Risikomanagements einer Organisation zu beziehen oder auf Zielkategorien, Komponenten, Organisationseinheiten oder jede Untermenge davon.



Funktionsfähigkeit

Beim Bestimmen, ob das unternehmensweite Risikomanagement einer Organisation funktionsfähig ist, wird ein Urteil auf Basis einer Bewertung des Vorhandenseins und der Wirksamkeit der acht Komponenten gefällt. Daher stellen die Komponenten auch Kriterien für ein funktionsfähiges unternehmensweites Risikomanagement dar. Damit diese Komponenten vorhanden und wirksam in Betrieb sind, darf keine wesentliche Schwäche vorliegen, und das Risiko muss im Bereich der Risikobereitschaft der Organisation liegen.

Falls das unternehmensweite Risikomanagement in allen vier Zielkategorien als funktionsfähig erachtet wird, haben das Überwachungs- und Leitungsorgan und die Führungskräfte hinreichende Sicherheit, dass sie die strategischen und betrieblichen Ziele erreichen, dass die Berichterstattung der Organisation zuverlässig ist und dass geltende Gesetze und Vorschriften eingehalten werden.

Die acht Komponenten werden nicht in jeder Organisation gleichartig aufgebaut sein. Die Umsetzung in kleinen und mittleren Organisationen mag zum Beispiel weniger formal und weniger strukturiert sein. Trotzdem können kleine Organisationen ein funktionsfähiges unternehmensweites Risikomanagement besitzen, so lange jede der Komponenten vorhanden und wirksam angewandt wird.

Einschränkungen

Während das unternehmensweite Risikomanagement bedeutende Vorteile bietet, unterliegt es auch Einschränkungen. Zusätzlich zu den oben besprochenen Faktoren entstehen praktische Beschränkungen daraus, dass die menschliche Urteilsbildung in Entscheidungsprozessen fehlerhaft sein kann, Entscheidungen über Risikoreaktionen und Kontrollmaßnahmen relative Kosten und Nutzen berücksichtigen müssen, Störungen allein aufgrund einfacher menschlicher Irrtümer oder Fehler eintreten können, Kontrollen durch Zusammenarbeit zweier oder mehrerer Personen umgangen werden sowie dass Führungskräfte Risikomanagemententscheidungen außer acht lassen. Diese Beschränkungen verhindern, dass Überwachungs- und Leitungsorgane sowie Führungskräfte vollständige Sicherheit bezüglich des Erreichens der Ziele der Organisation haben.

Interne Kontrolle einbeziehen

Die Interne Kontrolle ist ein integraler Bestandteil unternehmensweiten Risikomanagements. Dieses Rahmenwerk für unternehmensweites Risikomanagement beinhaltet Interne Kontrollen und bietet ein umfassenderes Konzept und Instrument für Führungskräfte. Die Internen Kontrollen werden in dem Rahmenwerk *Interne Kontrolle - Übergreifendes Rahmenwerk* definiert und beschrieben. Da sich dieses Rahmenwerk im Zeitablauf bewährt hat und Grundlage bestehender Regeln, Vorschriften und Gesetze ist, hat es weiterhin als Definition eines Rahmenwerks für Interne Kontrollen Bestand. Lediglich Teile des Textes aus der Veröffentlichung *Interne Kontrolle - Übergreifendes Rahmenwerk* werden wiederholt. Vielmehr ist dieses Rahmenwerk durch Bezugnahme in das hier vorliegende Rahmenwerk eingebunden.

Rollen und Verantwortlichkeiten

Jede Person in einer Organisation trägt einen Teil der Verantwortung für unternehmensweites Risikomanagement. Der Vorsitzende der Geschäftsleitung trägt die höchste Verantwortung und sollte dewegen die übergeordnete Zuständigkeit haben. Andere Führungskräfte stützen die Risikomanagementphilosophie der Organisation, fördern das Einhalten der Risikobereitschaft und steuern Risiken in ihrem Verantwortungsbereich unter Berücksichtigung der akzeptierten Risiken. Ein Risikomanager, Finanzleiter, Interner Revisor und andere haben im Normalfall unterstützende Aufgaben. Weitere Personen in der Organisation sind dafür verantwortlich, dass das unternehmensweite Risikomanagement unter Berücksichtigung vorgegebener Richtlinien und Verfahren durchgeführt wird. Das Überwachungs- und Leitungsorgan trägt eine bedeutende Überwachungsverantwortung für das unternehmensweite Risikomanagement; es kennt und hinterfragt die Risikobereitschaft der Organisation. Eine Gruppe externer Parteien, wie etwa Kunden, Lieferanten, Geschäftspartner, Abschlussprüfer, Aufsichtsinstanzen und Finanzanalysten, stellen häufig für die Durchführung des unternehmensweiten Risikomanagements nützliche Informationen zur Verfügung. Sie sind aber nicht verantwortlich für die Funktionsfähigkeit des unternehmensweiten Risikomanagements.

Aufbau dieses Berichts

Der Bericht gliedert sich in zwei Teile. Der erste Teil enthält sowohl das *Rahmenwerk* als auch eine *Zusammenfassung*. Das *Rahmenwerk* definiert das unternehmensweite Risikomanagement und beschreibt Prinzipien und Konzepte, enthält Anleitungen für alle Führungsebenen in Unternehmen und andere Organisationen zur Beurteilung und Verbesserung der Funktionsfähigkeit des unternehmensweiten Risikomanagements. Die *Zusammenfassung* ist eine Übersicht, die sich an die Geschäftsleitung, andere leitende Führungskräfte, Mitglieder von Überwachungs- und Leitungsorganen sowie Aufsichtsinstanzen wendet. Der zweite Teil, *Umsetzungsmethoden*, enthält beispielhafte Instrumente, die bei der Umsetzung der Elemente des Rahmenwerks nützlich sind.

Anwendung dieses Berichts

Maßnahmen, die auf Grundlage dieses Berichts und abhängig von der Stellung und der Rolle der beteiligten Parteien vorgeschlagen werden:

- *Überwachungs- und Leitungsorgan* - Das Überwachungs- und Leitungsorgan soll den Zustand des unternehmensweiten Risikomanagements mit den leitenden Führungskräften durchsprechen und wo erforderlich überwachend

eingreifen. Das Überwachungs- und Leitungsorgan soll sicherstellen, dass es über die wesentlichen Risiken, der von den Führungskräften ergriffenen Maßnahmen, sowie über darüberhinausgehende Risiken in Kenntnis gesetzt ist.

- *Leitende Führungskräfte* - Diese Untersuchung legt nahe, dass der Vorsitzende der Geschäftsleitung die Fähigkeit der Organisation zu unternehmensweitem Risikomanagement beurteilt. Ein Ansatz wäre, dass der Vorsitzende der Geschäftsleitung, Leiter von Geschäftsbereichen und wichtige funktional Verantwortliche zusammenkommen, um eine erste Beurteilung der Leistungs- und Funktionsfähigkeit des unternehmensweiten Risikomanagements zu erhalten. Wie auch immer dies geschieht, sollte eine erste Bewertung bestimmen, ob Bedarf zu einer zu vertiefenden Untersuchung besteht und wie dabei vorzugehen ist.
- *Andere Mitarbeiter* - Führungskräfte und andere Mitarbeiter sollen hinterfragen, wie sie ihrer Verantwortung vor dem Hintergrund dieses Rahmenwerks gerecht werden und mit höher gestellten Mitarbeitern ihre Vorschläge zur Verbesserung des unternehmensweiten Risikomanagements besprechen. Interne Revisoren sollen das Maß ihrer Ausrichtung auf das unternehmensweite Risikomanagement hinterfragen.
- *Aufsichtsinstanzen* - Dieses Rahmenwerk kann eine gemeinsame Betrachtung unternehmensweiten Risikomanagements fördern, einschließlich seiner Möglichkeiten und Beschränkungen. Aufsichtsinstanzen können sich auf dieses Rahmenwerk beziehen, wenn sie Erwartungen festlegen, sei es bei der Regelsetzung, in Empfehlungen oder beim Beurteilen der Organisationen, die sie beaufsichtigen.
- *Berufsverbände* - Regelsetzende oder andere berufsständische Organisationen, die Empfehlungen für Finanzmanagement, Prüfung und angrenzende Themenbereiche bereitstellen, sollten ihre Standards und Empfehlungen vor dem Hintergrund dieses Rahmenwerks abwägen. In dem Umfang, in dem die Abweichungen zwischen Konzepten und Fachtermini verringert werden, profitieren alle Beteiligten.
- *Forschung und Lehre* - Dieses Rahmenwerk kann Gegenstand von wissenschaftlicher Forschung und von Untersuchungen bezüglich zukünftiger Weiterentwicklungen sein. Unter der Annahme, dass dieser Bericht als allgemeine Verständigungsgrundlage Anerkennung finden wird, sollten auch seine Konzepte und Begriffe in die Unterichtspläne der Hochschulen Einzug halten.

Mit dieser Grundlage für ein gemeinsames Verständnis werden alle Beteiligen befähigt, eine einheitliche Sprache zu sprechen und wirksamer zu kommunizieren. Führungskräfte in Unternehmen werden befähigt, den unternehmensweiten Risikomanagementprozess ihres Unternehmens mit Hilfe eines Standards zu messen, diesen Prozess zu stärken und ihr Unternehmen hin zu den vorgegebenen Zielen zu entwickeln. Zukünftige Forschung kann auf der Basis einer vorhandenen Grundlage aufbauen. Gesetzgeber und Regulierungsinstanzen werden befähigt, ein vertieftes Verständnis von unternehmensweitem Risikomanagement einschließlich seines Nutzens und seiner Beschränkungen zu erlangen. Wenn alle Beteiligten ein gemeinsames Rahmenwerk für das unternehmensweite Risikomanagement nutzen, können diese Erfolge erreicht werden.

www.iir-ev.de

Das IIR ist ein gemeinnütziges Institut zur Förderung und Weiterentwicklung der Internen Revision in Deutschland. Es wurde 1958 gegründet und hat Mitglieder aus allen Bereichen der Wirtschaft, Wissenschaft und Verwaltung.

Das IIR unterstützt die für Prüfungs- und Beratungsaufgaben zuständigen Fach- und Führungskräfte in ihrer praktischen Arbeit. Fachkundige Persönlichkeiten aus Praxis und Wissenschaft tragen durch ihr vielfältiges Engagement zur Aufgabenerfüllung des IIR bei.

The Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance.

COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

The following five major professional associations established COSO in 1985: the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, The Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants).