Das Enterprise Risk Management (ERM) ist ein wichtiges Element der Corporate Governance. Es kann Unternehmen bei der Zielerreichung unterstützen, indem es hilft, Chancen und Risiken zu erkennen und geeignete Massnahmen zu ergreifen.

T. FLEMMING RUUD
KATERINA SOMMER

ENTERPRISE RISK MANAGEMENT
Das COSO-ERM-Framework

Die Weiterentwicklung des Internal-Control-Framework zu einem Enterprise-Risk-Management-Framework, dessen Grundsätze, Ziele und Komponenten, dessen Nutzen und Grenzen sowie die Unterschiede zum ursprünglichen COSO-IC-Framework ist Gegenstand der nachfolgenden Ausführungen.

1. ENTWICKLUNG

Die Rolle des Risikomanagements in Unternehmen hat sich in den letzten Jahren stark verändert. In der Vergangenheit hat sich das Risikomanagement auf finanzielle und versicherbare Risiken konzentriert und wurde häufig als Ad-hoc-Reaktion auf Ereignisse von einzelnen Abteilungen ausgeführt. Im Laufe der Zeit hat sich gezeigt, dass für das Risikomanagement eine breitere, unternehmensweite Perspektive notwendig ist, welche nicht nur finanzielle Risiken umfasst und als kontinuierlicher, proaktiver Prozess ausgestaltet ist – das ERM. Es wurde auch das Bedürfnis nach einem Framework zur effektiven Identifikation, Beurteilung und Handhabung von Risiken sichtbar. Das *Committee of Sponsoring Organizations of the Treadway Commission (COSO)* hat im Jahr 2004 das *Enterprise Risk Management – Integrated Framework* [1] *(COSO-ERM-Framework)* veröffentlicht. Dies fast ein Jahrzehnt nach der Veröffentlichung des *Internal Control – Integrated Framework* [2] *(COSO-IC-Framework)* [3], welches ein generell einsetzbares und in der Praxis das meist verwendete Konzept für die Gestaltung des internen Kontrollsystems darstellt [4]. Das COSO-ERM-Framework baut auf dem COSO-IC-Framework auf und erweitert den Fokus auf das ERM. Das COSO-ERM-Framework stellt ein unterstützendes Instrument zur Identifikation und Steuerung der Risiken im Rahmen der Risikobereitschaft des Unternehmens dar. Im zweiten Band *Enterprise Risk Management – Integrated Framework: Application Techniques* [5] werden illustrative Beispiele zur Anwendung des COSO-ERM-Framework auf unterschiedlichen Unternehmensebenen bereitgestellt.

2. COSO-ERM-FRAMEWORK

2.1 Definition. Das COSO-ERM trägt der gestiegenen Bedeutung des Risikomanagements hin zu einer ganzheitlichen und unternehmensweiten Betrachtung Rechung und definiert es wie folgt [6]:

«Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.»

Das ERM ist somit als fortdauernder Prozess zu verstehen, der durch Mitarbeitende aller Unternehmensebenen beeinflusst wird. Das ERM gelangt bereits bei der Festlegung der Unternehmensstrategie zum Zuge und ist darauf ausgerichtet, potentielle Ereignisse, die Einfluss auf das Unternehmen haben könnten, zu identifizieren, im Rahmen der Risikobereitschaft zu steuern und eine angemessene Zusicherung bezüglich der Unternehmenszielerreichung zu bieten. Somit baut das COSO-ERM-Framework auf den gleichen Grundsätzen wie das ursprüngliche COSO-IC-Framework auf und erweitert sie um zusätzliche risikobezogene Aspekte.

T. FLEMMING RUUD, PHD, WP (N), PROFESSOR FÜR WIRTSCHAFTSPRÜFUNG UND INTERNES AUDIT, UNIVERSITÄT ZÜRICH, STÄNDIGER GAST-PROFESSOR DER UNIVERSITÄT ST. GALLEN, ZÜRICH

KATERINA SOMMER, LIC. OEC. HSG, DOKTORANDIN UNIVERSITÄT ST. GALLEN, WISSENSCHAFTLICHE MITARBEITERIN VON PROF. T. FLEMMING RUUD, UNIVERSITÄT ZÜRICH, ZÜRICH

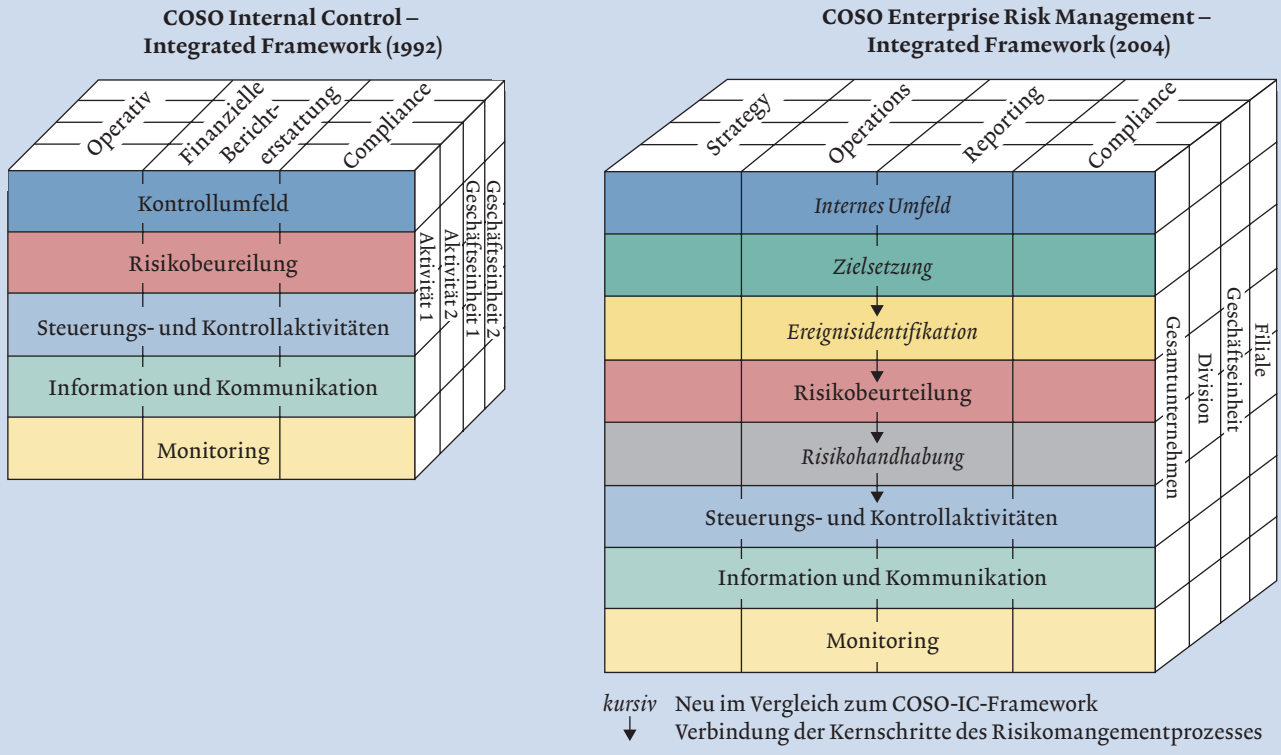
2.2 Ziele. Die allgemeine Zielsetzung des Risikomanagements ist die Erreichung einer optimalen Balance zwischen Risiko und Return (Renditeerwartung), nicht die Vermeidung aller potentiellen Risiken [7]. Das COSO-ERM-Framework unterstützt Unternehmen bei der Erreichung von Zielen in den folgenden vier Kategorien:
→ Strategic, d. h. übergeordnete Ziele, welche auf die Vision des Unternehmens abgestimmt sind und deren Umsetzung unterstützen; → Operations, d. h. Ziele, die sich auf die Effektivität und Effizienz der Geschäftsprozesse beziehen; → Reporting, d. h. Ziele, welche die Sicherstellung der Verlässlichkeit jeglicher Art von Berichterstattung beinhalten; → Compliance, d. h. Ziele, welche die Einhaltung von Gesetzen, Richtlinien und Normen umfassen.

Neu beim COSO-ERM-Framework sind gegenüber dem COSO-IC-Framework die Berücksichtigung der strategischen Ziele und die Ausdehnung der Berichterstattungsziele nicht nur auf die externe finanzielle Berichterstattung, sondern auf die Verlässlichkeit jeglicher Art von Informationen, d. h. finanzielle/nicht-finanzielle bzw. operationelle Informationen und interne/externe Berichterstattung [8].

2.3 Komponenten. Das COSO-ERM-Framework besteht aus acht Komponenten, welche einander wie folgt gegenseitig beeinflussen: Durch das Umfeld und die Anerkennung des ERM im Unternehmen werden die Grundlagen für das ERM geschaffen (Internes Umfeld). Die Festlegung der Ziele (Zielsetzung) ist notwendig, um diejenigen Ereignisse zu identifizieren, welche die Zielerreichung beeinträchtigen oder fördern können (Ereignisidentifikation). Auf dieser Basis können Risiken beurteilt (Risikobeurteilung) und entsprechende Massnahmen zu deren Steuerung evaluiert und ausgewählt werden (Risikohandhabung). Mittels Steuerungs- und Kontrollaktivitäten soll sichergestellt werden, dass diese Massnahmen auch umgesetzt werden (Steuerungs- und Kontrollaktivitäten). Wesentlich im ganzen Prozess ist die Dokumentation relevanter Informationen und deren Kommunikation auf allen vom ERM betroffenen Ebenen des Unternehmens (Information und Kommunikation). Um die Funktionsfähigkeit und Qualität des ERM sicherstellen zu können, muss es laufend beaufsichtigt und regelmässig überprüft werden (Monitoring) (vgl. *Abbildung 1*) [9].

2.3.1 Internes Umfeld. Die Komponente «Kontrollumfeld» des COSO-IC-Frameworks wurde auf «Internes Umfeld» im COSO-ERM-Framework ausgeweitet und bezieht sich somit neu auf das gesamte Unternehmen. Das Interne Umfeld bildet die Basis des Risikomanagementprozesses und beeinflusst alle anderen Komponenten. Es verleiht dem Unternehmen «discipline and structure» [11], d. h. eine Struktur, die durch folgende Faktoren beschrieben werden kann: Risikomanagementphilosophie spiegelt die Vorstellung des Unternehmens über Risiken und deren Handhabung wieder. Risikobereitschaft dient als Wegweiser bei der Strategiefestlegung im Hinblick auf das akzeptierbare Risiko bei der Strategieumsetzung. Von entscheidender Bedeutung ist die Zusammensetzung des Verwaltungsrats, denn ein starkes Internes Umfeld verlangt einen kompetenten, erfahrenen und unabhängigen Verwaltungsrat, der seine Oberaufsichts- und Ober-

Abbildung 1: **COSO-IC-FRAMEWORK UND COSO-ERM-FRAMEWORK IM VERGLEICH** [10]



leitungspflichten wahrnimmt. Die Integrität des Managements, der «tone at the top» und das Bekenntnis zu ethischen Werten ist geprägt durch Unternehmensgeschichte und -kultur und nimmt Einfluss auf das Verhalten der einzelnen Mitarbeitenden und somit das Unternehmen als Ganzes. Um die auferlegten Aufgaben erfüllen zu können, müssen die Mitarbeitenden über das notwendige Wissen und Fähigkeiten verfügen. Die Unternehmensstruktur bildet einen Rahmen für die Planung, Durchführung, Steuerung und Überwachung der Geschäftsaktivitäten. Sie definiert ebenfalls die Zuweisung von Autorität und Verantwortlichkeit. All diese Faktoren sollten sich auch im Umgang mit den Mitarbeitenden niederschlagen (vgl. *Abbildung 2*).

Das Ausmass der Umsetzung der einzelnen Komponenten unterscheidet sich je nach Unternehmen und Unternehmensgrösse. Auch wenn bei KMU die Formalisierung der Verantwortlichkeiten oder der Abläufe meistens gering ist, vermag auch ein starkes informelles Internes Umfeld eine angemessene Basis für das ERM zu bilden.

Während im COSO-IC-Framework der Risikomanagementaspekt mehr oder weniger implizit in der Komponente «Risikobeurteilung» enthalten ist, erweitert das COSO-ERM-Framework diesen Aspekt durch die Schaffung der Komponenten «Zielsetzung», «Ereignisidentifikation» und «Risikohandhabung», welche mit der Komponente «Risikobeurteilung» die Kernschritte des Risikomanagementprozesses bilden.

2.3.2 Zielsetzung. Das ERM gewährleistet das Vorhandensein eines Prozesses, welcher die Vereinbarkeit der gewählten Unternehmensziele mit der Vision und mit der festgelegten Risikobereitschaft sicherstellt. Die auf die Vision abgestimmten strategischen Ziele bilden die Grundlage für die abgeleiteten Zielsetzungen: Operative, Reporting- und Compliance-Ziele. Trotz einer teilweisen Überschneidung der Zielkategorien erlaubt diese Gliederung eine Fokussierung auf die einzelnen Aspekte des ERM sowie die meist unterschiedlichen operativen Verantwortlichkeiten. Da grundsätzlich erst nach der Zielsetzung die der Zielerreichung abträglichen Ereignisse identifiziert, beurteilt und dagegen Massnahmen ergriffen werden können, bildet die Komponente «Zielsetzung» den Ausgangspunkt des Risikomanagementprozesses und die Voraussetzung für die nachfolgenden vier Komponenten des COSO-ERM-Framework (vgl. Abbildung 2, auch für die nachfolgenden Komponenten).

2.3.3 Ereignisidentifikation. Bei der Identifikation von potentiellen Ereignissen mit positivem oder negativem Einfluss auf die Strategieumsetzung und Zielerreichung sind externe und interne sowie vergangene und zukünftige Faktoren zu berücksichtigen. Zu den externen Faktoren zählen ökonomische, ökologische, politische, soziale und technologische Einflüsse. Interne Faktoren beziehen sich auf die Fragen der Infrastruktur, des Personals, der Geschäftsprozesse oder der verwendeten Technologie. Ereignisse mit einem potentiell positiven Einfluss können negative Auswirkungen einschränken oder aufheben und gleichzeitig auch Chancen darstellen. Das Abschöpfen derartiger Chancen sollte in den Zielsetzungsprozess aufgenommen werden. Ereignisse mit einem potentiell negativen Einfluss (Risiken) sind zu beurteilen und es ist eine adäquate Reaktion darauf zu suchen. Die Kategorisierung der Ereignisse kann Basis der Risikoanalyse bilden und zum Verständnis der Zusammenhänge beitragen.

2.3.4 Risikobeurteilung. Die Risikobeurteilung erlaubt eine Einschätzung, welchen Einfluss potentielle Ereignisse auf die Erreichung der Unternehmensziele haben können. Dazu werden deren Eintrittswahrscheinlichkeit und Auswirkung eingeschätzt. Eine Risikobeurteilung erfolgt zuerst auf Basis des inhärenten Risikos, d.h. desjenigen Risikoniveaus vor der Massnahmenergreifung. Sobald eine Massnahme zur Steuerung der identifizierten Risiken ausgearbeitet wurde, erfolgt eine erneute Risikobeurteilung auf Basis des Residualrisikos, d. h. auf Basis des nach dem Ergreifen entsprechender Massnahmen verbleibenden Restrisikos. Bei der Risikoanalyse kann auf intern und/oder extern generierte Daten, Erfahrungswerte und/oder subjektive Schätzungen zurückgegriffen werden. Die Methodik zur Risikobeurteilung umfasst meistens eine Kombination von quantitativen und qualitativen Techniken. Tritt ein Ereignis nicht isoliert ein, sondern in einer Wechselbeziehung mit anderen Ereignissen, ist der Einfluss der Sequenz oder der Kombination von Auswirkungen zu beurteilen.

> *«Effektive Kommunikation erfolgt nicht nur über die Hierarchieebenen, sondern auch zwischen den organisatorischen Einheiten.»*

2.3.5 Risikohandhabung. Mögliche Massnahmen zur Handhabung von Risiken können in folgende vier Kategorien unterteilt werden: → Risikovermeidung durch Verzicht auf risikoinhärente Tätigkeiten; → Risikoreduktion durch Massnahmen zur Reduktion der Eintrittswahrscheinlichkeit, der Auswirkung oder Kombination der beiden; → Risikoteilung oder -überwälzung z. B. durch Versicherung oder Hedging; → Risikoübernahme durch bewusstes Nicht-Ergreifen von Massnahmen zur Handhabung von Risiken. Bei der Evaluation der Massnahmen sind deren Einfluss auf die Eintrittswahrscheinlichkeit und auf die potentielle Auswirkung sowie deren Kosten und Nutzen zu berücksichtigen. Bei der Auswahl kommen diejenigen Massnahmen in Frage, die das Residualrisiko auf das gewünschte Niveau reduzieren und innerhalb der Risikotoleranzwerte halten. Im Rahmen des ERM ist die Portfoliosicht bzw. unternehmensweite Sicht entscheidend: Risiken auf der Stufe der einzelnen Geschäftseinheiten können sich durchaus in den massgeblichen Risikotoleranzwerten bewegen, zusammen betrachtet, kann jedoch die Risikotoleranzgrenze des Gesamtunternehmens

überschritten sein. Oder umgekehrt können sich gewisse Einzelrisiken im Gesamtunternehmen ausgleichen. Mit Hilfe der Portfoliosicht soll folglich mittels einer angemessenen Diversifikation von Risiken die Zielerreichung des Gesamtunternehmens im Rahmen der Risikotoleranzwerte unterstützt und das Risk-Return-Profile optimiert werden.

2.3.6 Steuerungs- und Kontrollmassnahmen. Steuerungs- und Kontrollmassnahmen helfen sicherzustellen, dass die getroffenen risikosteuernden Massnahmen richtig und zeitnah ausgeführt und dass Risiken innerhalb der definierten Toleranzwerte gehalten werden können. Damit soll die Wahrscheinlichkeit erhöht werden, dass die festgelegten Unternehmensziele erreicht werden. Steuerungs- und Kontrollaktivitäten sind auf allen Ebenen und in allen Funktionen eines Unternehmens anzutreffen. Sie sind somit direkt in Managementprozesse eingebunden und beinhalten in der Regel einerseits Richtlinien zur Festhaltung der Soll-Vorgaben und anderseits Verfahren zu deren Umsetzung. Steuerungs- und Kontrollaktivitäten hängen stark mit dem Umfeld des Unternehmens, der Komplexität der Tätigkeiten, der Branche und der Unternehmenskultur zusammen und werden deshalb je nach Unternehmen unterschiedlich ausgestaltet. Grundsätzlich kann zwischen folgenden Massnahmen unterschieden werden:
→ Lenkende Massnahmen sollen ein gewünschtes Verhalten fördern. → Präventive Massnahmen dienen dazu, ein unerwünschtes Ereignis oder Verhalten zu verhindern. → Detektive Massnahmen sollen ein unerwünschtes Ereignis oder Verhalten entdecken und korrektive Massnahmen einleiten [12]. Steuerungs- und Kontrollaktivitäten können folglich sogar als Massnahmen zur Handhabung von Risiken dienen. Da man sich heute weitgehend auf Informationssysteme verlässt, sind auch Steuerungs- und Kontrollmassnahmen speziell für Informationssysteme notwendig [13].

2.3.7 Information und Kommunikation. Für die Ereignisidentifikation, Risikobeurteilung und Ergreifung angemessener Massnahmen zur Risikohandhabung sind relevante externe und interne Informationen auf allen Ebenen des Unternehmens notwendig. Effektive Kommunikation erfolgt nicht nur über die Hierarchieebenen, sondern auch zwischen den organisatorischen Einheiten. Für ein effektives ERM ist es unabdingbar, dass Mitarbeitende ihre Rolle im ERM kennen und die Wechselbeziehung mit Aktivitäten anderer ERM-Beteiligten verstehen. Der Austausch von Informationen und die Kommunikation schliessen auch die wichtigsten Anspruchsgruppen (Kunden, Lieferanten, Anteilseigner usw.) mit ein (vgl. Abbildung 2, auch für die nachfolgende Komponente).

2.3.8 Monitoring. Mittels Monitoring sollen das Funktionieren und die Qualität des ERM sichergestellt werden, wobei es durch laufende oder separate Beurteilungen oder eine Kombination von beiden erfolgen kann. Laufende Beurteilungen sind in die operativen Abläufe integriert und bilden somit einen Bestandteil gewöhnlicher Managementaktivitäten. Die Häufigkeit und das Ausmass der separaten Beurteilungen

Abbildung 2: **ELEMENTE DER KOMPONENTEN**

Internes Umfeld
→ Risikomanagementphilosophie
→ Risikobereitschaft
→ Zusammensetzung des Verwaltungsrats
→ Integrität und ethische Werte
→ Bekenntnis zur Kompetenz
→ Organisationsstruktur
→ Festlegung von Verantwortlichkeit und Autorität
→ Human-Ressource-Standards
↓
Zielsetzung
→ Strategische Ziele
→ Abgeleitete Ziele (operative, Reporting- und Compliance-Ziele)
→ Risikobereitschaft
→ Risikotoleranz
↓
Ereignisindentifikation
→ Erkennen von Ereignissen
→ Einflussfaktoren
→ Methoden zur Ereigniserkennung
→ Chancen und Risiken
→ Wechselbeziehungen zwischen Ereignissen
→ Ereigniskategorien
↓
Risikobeurteilung
→ Inhärentes Risiko und Residualrisiko
→ Eintrittswahrscheinlichkeit und Auswirkung
→ Methoden zur Risikobeurteilung
→ Wechselbeziehungen zwischen Ereignissen/Risiken
↓
Risikohandhabung
→ Massnahmen zur Handhabung von Risiken
→ Evaluation möglicher Massnahmen
→ Beurteilung und Auswahl geeigneter Massnahmen
→ Portfolio-Ansatz
↓
Steuerungs- und Kontrollaktivitäten
→ Abstimmung der Steuerungs- und Kontrollaktivitäten mit den Massnahmen zur Handhabung von Risiken
→ Arten der Steuerungs- und Kontrollaktivitäten
→ Richtlinien und Verfahren
→ Steuerungs- und Kontrollaktivitäten für IT-Systeme
↓
Information und Kommunikation
→ Information
→ Kommunikation
↓
Monitoring
→ Kontinuierliches Monitoring
→ Separate Beurteilungen
→ Berichterstattung über Mängel

hängen insbesondere von der Effektivität des laufenden Monitoring ab. Die Mängel im ERM sollen der nächst höheren hierarchischen Ebene kommuniziert werden, in schwerwiegenden Fällen dem Top-Management bzw. dem Verwaltungsrat [14].

2.4 Drei Dimensionen des COSO-ERM-Framework. Das COSO-ERM-Framework wird als Modell mit den drei Dimensionen Ziele, Komponenten (was wird benötigt, um diese Ziele zu erreichen) und organisatorische Einheiten dargestellt (vgl. Abbildung 1). Die vier Zielkategorien stehen in einer direkten Beziehung zu den acht Komponenten, denn jede der acht Komponenten bezieht sich auf alle vier Zielkategorien: Z. B. werden finanzielle und nicht-finanzielle Informationen aus internen oder externen Quellen als ein Teil der Komponente «Information und Kommunikation» (horizontale Reihe) bei der Strategiefestlegung, bei der effektiven und effizienten Geschäftstätigkeit, bei der Berichterstattung und bei der Ermittlung, ob das Unternehmen alle relevanten Normen einhält (vertikale Spalten), benötigt. Auch gelten die vier Zielkategorien für jede der acht Komponenten: So sind für die Erreichung der operativen Ziele (vertikale Spalte) alle acht Komponenten (horizontale Reihen) anwendbar und nötig. Das COSO-ERM-Framework ist für das gesamte Unternehmen sowie die einzelnen organisatorischen Einheiten relevant [15].

2.5 Verhältnis sowie Relevanz der beiden Frameworks. Wie aus den oben genannten Ausführungen ersichtlich ist, weist das COSO-ERM-Framework im Hinblick auf den gesamten Aufbau, insbesondere auf die Grundsätze, die Ziele und die Komponenten viele Gemeinsamkeiten mit dem COSO-IC-Framework auf und kann als dessen Erweiterung betrachtet werden. Das COSO-ERM-Framework ersetzt somit nicht das COSO-IC-Framework, sondern das COSO-IC-Framework wird als ein integrierter Bestandteil des COSO-ERM-Framework betrachtet [16].

Mit den Sections 302 und 404 des *Sarbanes-Oxley Act (SOX)* hat das COSO-IC-Framework bzw. die Internal Control im Bereich der finanziellen Berichterstattung an Bedeutung gewonnen [17|. Die Integration des COSO-IC-Framework im COSO-ERM-Framework ermöglicht es, auch mit der Anwendung des COSO-ERM-Framework den gesetzlichen Anforderungen gerecht zu werden. Unternehmen könnten dieses Framework somit einsetzen, um sowohl den Anforderungen des Internal-Control-Systems gerecht zu werden als auch für den Ausbau in Richtung eines Enterprise-Risk-Managements [18]. Abzuwarten bleibt, ob auch das COSO-ERM-Framework dieselbe weltweite Akzeptanz wie das COSO-IC-Framework erlangen wird. Dafür spricht, dass das COSO-IC-Framework einen Bestandteil des COSO-ERM-Framework bildet und dass die regulatorischen Bestimmungen (insbesondere SOX) somit bereits einen grossen Teil des COSO-ERM-Framework akzeptieren. Ebenfalls können Unternehmen, die das COSO-IC-Framework bereits anwenden, auf das COSO-ERM-Framework umstellen, indem sie auf bereits Vorhandenem und Bewährtem aufbauen und diese erweitern. Erste Erfahrungen bei der Umsetzung des COSO-ERM-Framework zeigen, dass dessen Nutzen als wesentlich empfunden wird [19]. Vor allem Unternehmen, die vom SOX betroffen sind, werden langfristig ein Risikomanagement vorzuweisen haben, das den Ansprüchen eines allgemein anerkannten Framework genügt [20].

Ebenfalls im Rahmen des «New Basel Capital Accord» (Basel II) gewinnt das Risikomanagement in Unternehmen immer mehr an Bedeutung. Bei der Bestimmung der Kreditkonditionen bzw. der Ratings werden durch die Banken nicht nur Kredit- und Marktrisiken erfasst, sondern auch operationelle (unzulängliche interne Abläufe, mangelnde Personalqualität, Systemfehler) und andere Risiken. Ein effektives und effizientes ERM kann zur Steuerung solcher Risiken massgeblich beitragen und einen positiven Einfluss auf die Kreditkonditionen bzw. Kapitalkosten des Unternehmens ausüben.

3. FAZIT

Das ERM kann als ein wichtiges Element der Corporate Governance einen wesentlichen Beitrag zum Management der Risiken und zur Erreichung der Unternehmensziele leisten. Zur Einführung, Anpassung und Aufrechterhaltung eines unternehmensweiten Risikomanagements bietet sich das COSO-ERM-Framework als internationale Richtlinie an. Es führt zu einer objektivierten Darstellung des komplexen ERM-Prozesses und zu einem vertieften Verständnis der Hauptrisiken, deren Auswirkungen und zu einer strukturierten Vorgehensweise beim Management von Risiken im Rahmen einer bewussten Risikoübernahme. Das gemeinsame Verständnis über die Inhalte des ERM erlaubt eine verbesserte Kommunikation zwischen den Beteiligten und erleichtert zudem eine unabhängige Beurteilung des ERM. Allerdings kann auch ein wirksames ERM nur eine angemessene Zusicherung bezüglich der Unternehmenszielerreichung bieten. Die Zielerreichung ist beeinflusst durch inhärente Beschränkungen, welche jedem Managementprozess innewohnen, wie beispielsweise Fehler und bewusstes Umgehen von Steuerungs- und Kontrollmassnahmen durch Absprache mehrerer Individuen usw. Heutzutage sind nicht nur das Management von Risiken und die Ausschöpfung von Chancen zu einer Überlebensnotwendigkeit geworden, sondern auch regulatorische Bestimmungen, Aktionäre und andere Stakeholder erwarten zunehmend die Einführung eines Risikomanagementsystems. Mit der Implementierung eines anerkannten Framework für ganzheitliches und systematisches Risikomanagement kann die Qualität des ERM auch nach aussen signalisiert werden. ■

Anmerkungen: 1) Vgl. COSO (2004a). Das kostenlose Executive Summary des COSO-ERM-Framework und das kostenpflichtige vollständige COSO-ERM-Framework sind erhältlich u. a. unter: http://www.coso.org/publications.htm. **2)** Vgl. COSO (1992). **3)** Das «Internal Control – Integrated Framework» wird in der Praxis als COSO-Modell bezeichnet. Damit es zu keinen Verwechslungen der beiden Frameworks kommt (beide wurden vom Committee of Sponsoring Organizations of the Treadway Commission (COSO) herausgegeben), wird in diesem Artikel für das «Internal Control – Integrated Framework» die Abkürzung COSO-IC-Framework und für das «Enterprise Risk Management – Integrated Framework» die Abkürzung COSO-ERM-

Framework verwendet. **4)** Das COSO hat im Oktober 2005 einen Entwurf unter dem Namen «Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting» publiziert, welcher die Anwendung des COSO-IC-Framework für kleinere Publikumsgesellschaften veranschaulichen soll. **5)** Vgl. COSO (2004b). **6)** COSO (2004a), S. 4. **7)** Nicht die Übernahme von allen Risiken führt zu einer höheren (risikobereinigten) Rendite. Nur für die Übernahme von nicht-diversifizierbaren (systematischen) Risiken kann eine Prämie als Renditevorteil erwartet werden. Da für die Übernahme von diversifizierbaren (unsystematischen) Risiken keine Renditeprämie erwartet werden kann, ist eine Portfoliosicht bzw. ein ganzheitliches Risikomanagement angebracht. Bei einer konservativen Risikopolitik werden Risiken zwar weitgehend vermieden, gleichzeitig wird aber auch zugunsten von Sicherheit auf Chancen verzichtet («no risk, no return»). Der Umkehrschluss, dass im Rahmen einer aggressiven Risikopolitik die Übernahme von mehr Risiko zu mehr Renditeerwartung führt, wäre jedoch aus den oben erwähnten Gründen nicht angebracht. Im Rahmen einer optimalen Risikopolitik soll die angestrebte Balance zwischen Risiko und Renditeerwartung (Return) erreicht werden. **8)** Vgl. COSO (2004a), S. 5 und 109–110. **9)** Für die nachfolgenden Ausführungen zu den Komponenten des COSO-ERM-Framework vgl. COSO (2004a), S. 5–6, 27–81. **10)** In Anlehnung an COSO (1992), S. 19 und COSO (2004a), S. 23. Das COSO-IC-Framework kann auch als eine Pyramide dargestellt werden, vgl. COSO (1992), S. 17. **11)** COSO (2004a), S. 27. D. h. «Internes Umfeld» beeinflusst, wie Strategie und Ziele festgelegt, wie Geschäftsaktivitäten strukturiert und wie Risiken identifiziert, beurteilt und behandelt werden. Zudem nimmt es Einfluss auf die Ausgestaltung und Funktionsweise der Steuerungs- und Kontrollaktivitäten, der Informations- und Kommunikationssysteme sowie der Monitoring-Aktivitäten. **12)** Vgl. The IIA (2004a), PA 2100-1: Art der Arbeiten, Ziff. 6 und Ruud/Jenal (2005), S. 456. **13)** Hierzu gehören einerseits generelle Kontrollen, die das IT-Management, die IT-Infrastruktur, das Sicherheitsmanagement und die Software-Beschaffung, Entwicklung und Wartung betreffen. Andererseits sind es Applikationskontrollen, welche die Vollständigkeit, Fehlerfreiheit, Autorisierung und Gültigkeit von Daten im Rahmen einzelner Applikationen sicherstellen sollen. **14)** Das Monitoring des ERM gehört zu den primären Aufgaben des internen Audits in bezug auf das Risikomanagement. Vgl. dazu COSO (2004a), S. 75–81 und The IIA (2004b). Zur Rolle des internen Audits im ERM vgl. den Artikel der Autoren in der nächsten Ausgabe des ST. **15)** Vgl. COSO (2004a), S. 7 und 23–24. **16)** Vgl. COSO (2004a), S. 109–112. **17)** Das COSO-IC-Framework wird als anerkannte Grundlage für die periodische Beurteilung des Internal-Control-Systems über die finanzielle Berichterstattung in den Ausführungsverordnungen der Securities and Exchange Commission zum Sarbanes-Oxley Act erwähnt. Vgl. SEC Final Rule, Release Nos. 33–8238; 34–47986, II.B.3.a. **18)** Vgl. COSO (2004a), S. v. **19)** Vgl. Conference Board (2005). **20)** Vgl. The IIA (2005), o.S., Chapman (2003), S. 33, Moeller (2004), S. 232 und 237.

Literatur: ▶ Chapman, Christy (2003): Bringing ERM into Focus, in: Internal Auditor, Juni 2003, Vol. 60, Issue 3, S. 30–35. ▶ Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992): Internal Control – Integrated Framework. Jersey City, New Jersey, 1992. ▶ Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004a): Enterprise Risk Management – Integrated Framework: Executive Summary, Framework, Jersey City (NJ), 2004. ▶ Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004b): Enterprise Risk Management – Integrated Framework: Application Techniques, Jersey City (NJ), 2004. ▶ Conference Board (2005): From Risk Management to Risk Strategy. Abrufbar im Internet unter: http://www.conference-board.org/publications/describe.cfm?id=1033, Stand: 5. Dezember 2005. ▶ Moeller, Robert (2004): Sarbanes-Oxley and the New Auditing Rules, John Wiley & Sons, New Jersey, 2004. ▶ SEC Final Rule, Release Nos. 33–8238, 34–47968: Management's Report on Internal Control over Financial Reporting and Certification Disclosure in Exchange Act Periodic Reports. Abrufbar im Internet unter: http://www.sec.gov/rules/final/33–8238.htm. Stand 5. Dezember 2005. ▶ Ruud, Flemming T./Jenal, Ladina (2005): Licht im Internal-Control-Dschungel, in: Der Schweizer Treuhänder, 6–7/2005, S. 455–460. ▶ The Institute of Internal Auditors (The IIA) (2004a): The Professional Practices Framework, Altamonte Springs (FL), 2004. Für die offizielle deutsche Übersetzung: Der Institut für Interne Revision e. V. (2005): Standards für die berufliche Praxis der Internen Revision, 2005. ▶ The Institute of Internal Auditors (The IIA) (2004b): Position Statement – The Role of Internal Audit in Enterprise-wide Risk Management. Abrufbar im Internet unter: http://www.theiia.org/download.cfm?file=25663, Stand: 5. Dezember 2005. ▶ The Institute of Internal Auditors (The IIA) (2005): FAQ for COSO's Enterprise Risk Management – Integrated Framework. Abrufbar im Internet unter: http://www.theiia.org/index.cfm?doc_id=4883, Stand: 5. Dezember 2005.

RESUME

Gestion des risques dans l'entreprise

Le Committee of Sponsoring Organizations of the Treadway Commission a publié en 2004 l'*«Enterprise Risk Management – Integrated Framework» (COSO ERM)*. Le COSO ERM aide les entreprises à réaliser leurs objectifs dans les catégories Strategic, Operations, Reporting et Compliance. Il s'agit de huit modules interagissant de la manière suivante: l'environnement général et la reconnaissance de l'ERM dans l'entreprise créent les bases de l'ERM («Environnement interne»). La définition des objectifs («Objectifs») est indispensable pour identifier les événements susceptibles d'entraver ou de favoriser la réalisation des objectifs («Identification des événements»). Partant de là, il est possible de procéder à une évaluation des risques («Évaluation des risques»), puis d'évaluer et de sélectionner les mesures aptes à les piloter («Gestion des risques»). Le but des activités de pilotage et de contrôle est de garantir que ces mesures soient effectivement appliquées («Activités de pilotage et de contrôle»). Consigner par écrit les informations importantes et les transmettre à tous les niveaux de l'entreprise concernés par l'ERM est un des aspects essentiels de cette procédure («Information et communication»). Afin d'en garantir le bon fonctionnement et la qualité, l'ERM doit faire l'objet d'une surveillance constante et de contrôles réguliers («Surveillance»). Le COSO ERM est important pour l'ensemble de l'entreprise ainsi que pour les différentes entités organisationnelles. Il peut dès lors être modélisé en trois dimensions: objectifs, composantes et entités organisationnelles.

En tant qu'élément important de la gouvernance d'entreprise, l'ERM peut apporter une contribution majeure à la gestion des risques et à la réalisation des objectifs de l'entreprise. Le référentiel COSO ERM, à titre de directive internationale, convient parfaitement dès lors qu'il s'agit de mettre en place ou de maintenir un système de gestion du risque dans l'ensemble d'une entreprise. Il permet une présentation objectivisée d'une procédure ERM complexe, une connaissance approfondie des principaux risques et de leur impact ainsi qu'une approche structurée de la gestion des risques et de les assumer en toute connaissance de cause. De nos jours, la gestion du risque et l'exploitation des opportunités ne sont pas uniquement des facteurs de survie de l'entreprise; elles sont devenues des dispositions régulatives et les actionnaires et autres parties prenantes exigent de plus en plus souvent l'introduction d'un système de gestion des risques. La mise en place d'un cadre reconnu de gestion globale et systématique des risques permet en outre de faire connaître à l'extérieur de l'entreprise la qualité de l'ERM pratiquée par cette dernière.

TFR/KS/JA