

Das Enterprise Risk Management (ERM) unterstützt das Unternehmen beim Umgang mit Risiken und dadurch bei der Erreichung von Unternehmenszielen. Das interne Audit kann zum effektiven und effizienten ERM auf vielfältige Weise mit Assurance- und Beratungsdienstleistungen beitragen. Das ERM bietet wiederum Input für die Tätigkeiten des internen Audits.

T. FLEMMING RUUD

KATERINA SOMMER

INTERNES AUDIT UND ENTERPRISE RISK MANAGEMENT

Enterprise Risk Management in der Praxis

1. EINLEITUNG

Die Aufgabe des internen Audits im Bereich des Risikomanagements ist bereits in der Definition des internen Audits sichtbar: Das interne Audit hat mittels objektiver und unabhängiger Assurance- und Beratungsdienstleistungen die Organisation bei der Erreichung ihrer Ziele zu unterstützen, indem es mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der internen Steuerung und Kontrolle sowie der Governance-Prozesse beurteilt und diese verbessern hilft [1].

Das *Enterprise Risk Management (ERM)* steht mit dem internen Audit in einer Wechselbeziehung: Einerseits beurteilt das interne Audit das Risikomanagementsystem des Unternehmens, andererseits können die Informationen aus dem ERM Grundlage für die Tätigkeit des internen Audits bieten. Umgekehrt ist es sinnvoll, die Prüfungsergebnisse des internen Audits in die Risikobeurteilung im Rahmen des ERM einzubeziehen. Die möglichen Rollen des internen Audits im ERM, deren Konsequenzen sowie der Einfluss des ERM auf die Tätigkeiten des internen Audits werden nachstehend dargestellt.

2. ROLLE DES INTERNEN AUDITS IM ERM

Die Verantwortung für das Risikomanagement obliegt dem Verwaltungsrat, in der Praxis werden aber die diesbezüglichen operativen Aufgaben meistens an das Management delegiert [2]. Die Kernaufgabe des internen Audits in Bezug auf das Risikomanagement ist die Unterstützung des Verwaltungsrats bzw. des Managements, indem es die Angemessenheit und die Wirksamkeit der Risikomanagementprozesse

untersucht, bewertet, darüber Bericht erstattet und Verbesserungen vorschlägt [3]. Die primäre Aufgabe des internen Audits in Bezug auf das ERM besteht somit in der Erbringung von Assurance-Dienstleistungen. Die Einrichtung und die laufende Pflege des ERM liegen hingegen aufgrund der Problematik im Zusammenhang mit der Unabhängigkeit und Objektivität nicht im primären Verantwortungsbereich des internen Audits. Ist der Leiter des internen Audits der Auffassung, dass nur ungenügende Massnahmen ergriffen oder die Massnahmen unzulänglich umgesetzt wurden, so dass es zur Übernahme eines untragbaren Restrisikos für das Unternehmen führen könnte, hat er dies gemäss dem IIA-Standard 2600 mit der Geschäftsleitung zu besprechen. Kommt dabei keine Übereinstimmung zustande, hat er den Sachverhalt dem Verwaltungsrat darzulegen [4].

Aufgrund der Aktualität des Themas hat das *Institute of Internal Auditors (IIA)* nach der Veröffentlichung des COSO-ERM-Framework ein Position Statement *The Role of Internal Audit in Enterprise-wide Risk Management* [5] herausgegeben. Es zeigt auf, wie interne Auditoren die von den IIA-Standards geforderte Unabhängigkeit und Objektivität bei der Durchführung der Assurance- und Beratungsdienstleistungen im Bereich des ERM sicherstellen können. Bei der Bestimmung der Rolle des internen Audits in Bezug auf das ERM ist zu berücksichtigen, ob solche Aktivitäten die Unabhängigkeit und Objektivität des internen Audits beeinträchtigen und ob es wahrscheinlich ist, dass diese Aktivitäten die Risikomanagement-, Steuerungs- und Kontroll- sowie Governance-Prozesse verbessern können.



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

2.1 Kernaktivitäten. Zu den Kernaktivitäten des internen Audits in bezug auf das ERM zählen Assurance-Dienstleistungen wie [6]:

- Assurance bezüglich Risikomanagementprozesse; → Assurance bezüglich der korrekten Evaluation von Risiken;
- Beurteilung der Risikomanagementprozesse; → Beurteilung der Berichterstattung über die Hauptrisiken; → Review der Handhabung der Hauptrisiken.

Das interne Audit kann auch Beratungsdienstleistungen im Bereich des ERM erbringen. Das Ausmass ist abhängig von

«Die primäre Aufgabe des internen Audits in bezug auf das ERM besteht somit in der Erbringung von Assurance-Dienstleistungen.»

der Verfügbarkeit anderer externer und interner Ressourcen sowie von dem sich im Laufe der Zeit verändernden Reifegrad des ERM im Unternehmen. Insbesondere bei der Einführung eines ERM ist die Expertise des internen Audits bei der Beurteilung von Risiken und beim Verständnis deren Wechselbeziehungen nützlich. Es ist deshalb möglich, dass das interne Audit auf Verlangen in der Einführungsphase auch eine proaktive Rolle im ERM übernehmen könnte [7]. Mit zunehmender Einbettung des ERM im Unternehmen kann das Engagement des internen Audits reduziert werden.

2.2 Legitime Aktivitäten mit Schutzmassnahmen. Bei der Prüfung der Vereinbarkeit der Beratungs- mit den Assurance-Dienstleistungen ist entscheidend, ob die internen Auditoren Managementverantwortung übernehmen. Das interne Audit kann seine Einbindung im ERM über die Assurance-Dienstleistungen ausweiten, so lange es keine Verantwortung für das Management der Risiken übernimmt und gewisse Schutzvorkehrungen gewahrt bleiben. Dazu gehören folgende Aktivitäten:

- Erleichterung der Identifikation und Evaluation von Risiken (Beratung, Moderation von Workshops, Schulung, Schaffung eines gemeinsamen Verständnisses usw.); → Coaching des Managements betreffend der Handhabung von Risiken; → Koordination der ERM-Aktivitäten; → Konsolidierung der Berichterstattung über Risiken; → Entwicklung und Aufrechterhaltung des ERM-Frameworks; → Verfechtung der Einrichtung des ERM [8].

Je weiter unten in der Aufzählung die Tätigkeit des internen Audits aufgelistet ist, desto stärker sollen die Schutzmassnahmen sein. Unter den erwähnten Schutzmassnahmen ist Folgendes zu verstehen: Es sollte klargestellt werden, dass der Verwaltungsrat bzw. das Management für das ERM verantwortlich ist und bleibt. Die Art der Verantwortung des internen Audits betreffend ERM sollte im Audit Charter do-

kumentiert sein und vom Audit Committee genehmigt werden. Das interne Audit sollte keine Risiken im Namen des Managements steuern, keine diesbezüglichen Entscheidungen treffen und keine Verantwortung für das ERM übernehmen. Es kann beratend tätig sein, das ERM fördern und das Management im Bereich des Risikomanagements unterstützen. Grundsätzlich soll alles, was über Assurance-Dienstleistungen hinausgeht, als Beratungsdienstleistung aufgefasst werden, wobei die entsprechenden Standards anzuwenden sind.

2.3 Nicht empfohlene Aktivitäten. Für folgende Aktivitäten mit Bezug auf das ERM, welche über die normalen Assurance- und Beratungsdienstleistungen hinausgehen, wird vom IIA empfohlen, dass sie nicht vom internen Audit durchgeführt werden sollen, weil sie ihre Objektivität und Unabhängigkeit beeinträchtigen können:

- Bestimmung der Risikobereitschaft des Unternehmens;
- Einführung von Risikomanagementprozessen; → Treffen

KARRIEREWEGE DER INTERNEN AUDITOREN – EINE EMPIRISCHE ANALYSE IN DER SCHWEIZ

Was wissen Sie über Ihre Karrieremöglichkeiten als interner Auditor?

Inwiefern können/konnten Sie das interne Audit als Karrieresprungbrett nutzen?

Welche Karrieremöglichkeiten gibt es für internen Auditoren ausserhalb des internen Audits?

Welche (typischen) Karrierewege existieren in diesem Berufsfeld in der Schweiz?

Wie wird sich der interne Audit-Markt mittelfristig entwickeln?

Im Rahmen einer Diplomarbeit an der Universität Zürich bei Prof. T. F. Ruud, PhD, wird solchen Fragestellungen nachgegangen. Anhand einer schweizweiten Umfrage soll untersucht werden, welche Karrierewege interne Auditoren verschiedener Branchen innerhalb dieses Berufsfelds und anschliessend einschlagen können. Zusätzlich wird mit dem Resultat auch eine aktuelle Situationsanalyse mit Ausblick in die Zukunft erarbeitet.

Umfrageaufruf für aktive und ehemalige interne Auditoren

Sie sind interner Auditor oder früher in diesem Bereich tätig gewesen? Dann sind Sie herzlich eingeladen, an der Umfrage teilzunehmen! Sie dauert etwa 15 Minuten und kann auf folgender Webseite gestartet werden:

<http://www.InternalAudit.ch>

Die Umfrage dauert bis zum 23. April 2006. Die Ergebnisse werden Ende Mai 2006 auf der oben genannten Homepage veröffentlicht.

Andri Arn, Student der Universität Zürich

von Entscheidungen betreffend die Massnahmen zur Risikohandhabung; → Implementierung der Massnahmen zur Risikohandhabung im Namen des Managements; → Übernahme der Verantwortung für das ERM.

Die Beeinträchtigung der Objektivität und Unabhängigkeit ist dann den entsprechenden Stellen offenzulegen, wobei die Art der Offenlegung von der jeweiligen Beeinträchtigung abhängt [9].

Das Position Statement des IIA hat zu Diskussionen geführt, wie diese Empfehlung umzusetzen ist. Letztendlich obliegt es aber den einzelnen Unternehmen, die Rolle des internen Audits im Risikomanagementprozess zu bestimmen und diese Verantwortung allenfalls dem internen Audit zu übertragen. Dies hängt von Faktoren wie Unternehmenskultur und -grösse, Fähigkeiten der internen Auditoren, Verfügbarkeit von bzw. Mangel an anderen Ressourcen sowie kulturellen Gegebenheiten des Unternehmens ab [10].

3. EINFLUSS DES ERM AUF DIE TÄTIGKEIT DES INTERNEN AUDITS

Gemäss dem IIA-Standard 2010.A1 hat die Prüfungsplanung des internen Audits auf Basis einer Risikobeurteilung zu erfolgen [11]. Diese Vorgehensweise bei der Prüfungsplanung ist normalerweise ein anderer Prozess als bei der Risikobeurteilung im Rahmen des ERM. Bei einer «traditionellen» risikoorientierten Prüfungsplanung ist der Fokus mehr auf die Prüfungs- und weniger auf die Geschäftsrisiken ausgerichtet. Beim Vorhandensein eines ERM im Unternehmen bietet es sich an, die Informationen aus dem ERM-Prozess in die Risikobeurteilung bei der Prüfungsplanung und in die Prüfungsdurchführung einzubeziehen (risikobasiertes internes Auditing). Der Hauptunterschied besteht darin, dass im Rahmen des risikobasierten internen Auditing der Fokus auf das Verständnis und die Analyse der Risikobeurteilung des Ma-

agements gerichtet ist und dass der Prüfungsprozess auf der Risikobeurteilung des Managements aufbaut. Eine solche Vorgehensweise bzw. der Einbezug der Informationen aus dem ERM in die Prüfungsplanung und -durchführung ist jedoch abhängig vom Stadium der Implementierung des ERM im Unternehmen bzw. dem angestrebten Implementierungsgrad des ERM (nicht alle Unternehmen wollen z. B. aus Kosten-Nutzen-Überlegungen das ERM überhaupt oder so weitreichend implementieren). Zur Einführung bzw. Anpassung und Aufrechterhaltung eines unternehmensweiten Risikomanagements bietet sich das *Enterprise Risk Management – Integrated Framework* [12] COSO ERM-Framework an.

Bei weniger entwickelten Risikomanagementsystemen, die keine oder nur unzureichende Prozesse zur Identifikation, Beurteilung und Steuerung von Risiken enthalten, kann sich das interne Audit nicht auf die Risikobeurteilung des Managements verlassen und hat aus diesem Grund eigene Risikobeurteilungen vorzunehmen. Bei ausgereifteren Risikomanagementsystemen kann das interne Audit die Risikobeurteilungen des Managements in zunehmendem Masse verwenden bzw. der eigenen Risikobeurteilung gegenüberstellen, wobei eine kritische Hinterfragung angebracht ist. Das Ausmass, in welchem sich das interne Audit auf die Risikobeurteilung des Managements verlassen kann bzw. in welchem es eigene Beurteilungen vornehmen muss, ist auch von anderen Faktoren, wie z. B. der Geschwindigkeit der Veränderungen in der Organisationsstruktur und Unternehmensstrategie, abhängig (vgl. *Abbildung*).

Ein risikobasiertes internes Auditing trägt dazu bei, dass die Ressourcen des internen Audits in den für das Unternehmen wichtigsten Bereichen eingesetzt werden. Diese Vorgehensweise ermöglicht eine direkte «Verbindung» des internen Audits mit dem Risikomanagement, wodurch Synergien geschaffen, Doppelspurigkeiten reduziert, Gesamtzusammenhänge berücksichtigt und die Effektivität und Effizienz des

Abbildung: **ENTWICKLUNGSSTADIUM DES RISIKOMANAGEMENTS UND MÖGLICHE VORGEHENSWEISEN** [13]

Entwicklungsstadium des Risikomanagements Charakteristik	Mögliche Vorgehensweisen des internen Audits
Risk naïve Keine Formalisierung des Risikomanagements	→ Förderung eines Risikomanagements → Vornehmen von eigenen Risikobeurteilungen
Risk aware «Zerstreutes» bzw. für einzelne Bereiche des Unternehmens isoliertes Risikomanagement	→ Förderung eines unternehmensweiten Risikomanagements (ERM) → Vornehmen von eigenen Risikobeurteilungen
Risk defined Strategie und Richtlinien sind vorhanden und werden kommuniziert, Risikobereitschaft ist definiert	→ Förderung und Erleichterung des unternehmensweiten Risikomanagements (ERM) → Verwendung der Risikobeurteilung des Managements, wo angemessen
Risk managed/risk enabled Unternehmensweites Risikomanagement (ERM) ist vorhanden und wird kommuniziert/ERM und Internal Control sind vollständig in die Tätigkeit des Unternehmens eingebettet	→ Prüfung der Risikomanagementprozesse → Verwendung der Risikobeurteilung des Managements, wo angemessen

internen Audits erhöht werden. Ebenfalls führt eine derartige Risikoorientierung des internen Audits zu einer höheren Akzeptanz der Prüfungen durch das Management, da Übereinstimmung über die Relevanz der geplanten Prüfungen besteht. Das ERM unterstützt somit die Arbeit des internen Audits. Umgekehrt können auch die so gewonnenen Prüfungsergebnisse wiederum in die Risikobeurteilung im Rahmen des ERM mit einbezogen werden [14].

4. DAS ERM IN DER PRAXIS

Zum Thema ERM wurden in den letzten Jahren verschiedene Studien durchgeführt [15]. Die neueste Studie untersucht das Stadium der Umsetzung des ERM, die Rolle des internen Audits im ERM und den Einfluss des ERM auf das interne Audit [16].

Bei der Untersuchung des Grades der Umsetzung des ERM hat sich ein breites Spektrum gezeigt: Lediglich 11% der befragten Unternehmen haben das ERM bereits vollständig, etwa 37% teilweise implementiert. Somit hat ungefähr die Hälfte der befragten Unternehmen das ERM bereits umgesetzt oder ist auf dem Weg dahin. Von der anderen Hälfte der Unternehmen mit keinem ERM plant etwa ein Drittel die Einführung eines ERM in der Zukunft, ein weiteres Drittel plant keine Umsetzung des ERM und bei einem Drittel der Unternehmen ist noch keine diesbezügliche Entscheidung gefallen.

Bei den Unternehmen mit einer vollständigen oder teilweisen Implementierung des ERM wurde die Rolle des internen Audits im ERM untersucht. In der Reihenfolge abnehmender Häufigkeit wurden folgende Aktivitäten angegeben:

→ Koordination der ERM-Aktivitäten; → Hilfestellung bei der Risikoidentifikation; → Vorschläge betreffend Steuerungs- und Kontrollaktivitäten; → Monitoring des ERM-Prozesses.

Am wenigsten wurde das interne Audit bei der Durchführung der Risikobeurteilung (Einschätzung der Eintrittswahrscheinlichkeit und Auswirkung) und der Identifikation der angemessenen Massnahmen zur Risikohandhabung involviert. Diese Ergebnisse decken sich mit der Forderung an die Unabhängigkeit und Objektivität des internen Audits.

Der Einfluss des ERM auf das interne Audit wurde insgesamt als moderat ausgewiesen. Qualitative Antworten betreffend den Einfluss ergaben zusammengefasst u. a. folgendes Bild: → Das ERM hat zum besseren Verständnis der Unternehmensrisiken seitens der internen Auditoren geführt, was wiederum Einfluss auf die Prüfungsplanung und -durchführung hat (z. B. Verschiebung der Prüfungsaktivitäten in Bereiche mit höherem Risiko); → Das ERM hat zu einem verbes-

serten Status des internen Audits im Unternehmen geführt; → Das ERM führte zu einer grösseren Arbeitsbelastung für das interne Audit.

Ein stärkeres Engagement des internen Audit im ERM fordern insbesondere der Chief Risk Officer (falls eine solche Position existiert), das Audit Committee und der Chief Financial Officer. Diese Parteien sind diejenigen mit einer starken Risikoorientierung und gleichzeitig diejenigen, mit denen das interne Audit am häufigsten zusammenarbeitet. Durchschnittlich wurden nur 7% der verfügbaren Zeit für das

«Das interne Audit steht mit dem ERM in einer Wechselbeziehung.»

Monitoring des ERM oder die Ausbildung im Bereich des ERM aufgewendet; der grösste Teil der Zeit wurde erwartungsgemäss mit operativen Audits (etwa 27%) und Audits der Internal Control im Bereich der finanziellen Berichterstattung gemäss dem *Sarbanes-Oxley Act* (etwa 18%) verbracht. Eine andere Studie hat gezeigt, dass lediglich bei einem Drittel der befragten Unternehmen das interne Audit mit dem ERM zusammenwirkt [17]. Aus diesen Studien ist einerseits grosse Heterogenität betreffend die Stadien der Umsetzung des ERM sichtbar geworden. Andererseits wurden die Vielfältigkeit der tatsächlichen Rolle des internen Audits im ERM sowie der erwartete vorwiegend positive Einfluss des ERM auf das interne Audit deutlich.

5. FAZIT

Das interne Audit kann einen wesentlichen Beitrag zum ERM leisten. Das Engagement des internen Audits im ERM ist primär abhängig von den Gegebenheiten jedes einzelnen Unternehmens. Es wird auch durch Überlegungen zur Unabhängigkeit und Objektivität geleitet und kann je nach Stadium der Umsetzung des ERM variieren. Das interne Audit steht mit dem ERM in einer Wechselbeziehung: Das interne Audit beurteilt die Risikomanagementprozesse und kann darüber hinaus gewisse Beratungsdienstleistungen erbringen. Informationen aus dem ERM können wiederum dem internen Audit Grundlage für seine Prüfungstätigkeit bieten. Die aus solchen Prüfungen gewonnenen Ergebnisse können in die Risikobeurteilung im Rahmen des ERM einfließen. Diese Synergiepotentiale gilt es zu nutzen, was allerdings heute nur in wenigen Unternehmen der Fall ist. ■

Anmerkungen: 1) Vgl. für die Definition des internen Audits The IIA (2004a), S. xxvii. 2) Das Schweizer Obligationenrecht äussert sich weder in der gültigen Fassung noch im Entwurf zur Änderung des Obligationenrechts unter den unübertragbaren Aufgaben des Verwaltungsrats explizit zur Verantwortung des Verwaltungsrats für das Risikomanagement. Sie ergibt sich aber indirekt aus Art. 716a

OR und Art. 716a E-OR (vgl. Bundesrat [2005]), denn der Verwaltungsrat ist für die Oberleitung der Gesellschaft zuständig, wozu auch das strategische Risikomanagement gehört. Auch der Swiss Code of Best Practice for Corporate Governance empfiehlt, dass der Verwaltungsrat für ein dem Unternehmen angepasstes Risikomanagement sorgt (vgl. Economiesuisse [2002], Ziff. 19). 3) Vgl. The

IIA (2004a): IIA-Standard 2110.A1: «Das Interne Audit überwacht und bewertet die Effektivität des Risikomanagementsystems der Organisation.» The IIA (2004a): Praktischer Ratschlag 2110-1: Beurteilung der Angemessenheit von Risikomanagementprozessen und The IIA (2004b), S. 4. 4) Vgl. The IIA (2004a): IIA-Standard 2600: Entscheidung über die Risikoübernahme durch das Manage-

ment. 5) Vgl. The IIA (2004b). Die nachfolgenden Ausführungen stützen sich auf dieses Position Statement und Jackson (2005), S. 44–50. 6) Für die entsprechenden Prüfungsverfahren und Zielsetzungen vgl. The IIA (2004a): PA 2110-1: Beurteilung der Angemessenheit von Risikomanagementprozessen. 7) Vgl. auch The IIA (2004a): PA 2100-4: Rolle des internen Audits in Organisationen ohne Risikomanagementprozess. 8) Das IIA zählt zu solchen Aktivitäten auch die Entwicklung einer durch den Verwaltungsrat zu genehmigenden Risikomanagementstrategie. Dabei ist nach Auffassung der Autoren die Gefahr bereits gross, dass dadurch die Unabhängigkeit und Objektivität gefährdet werden. 9) Vgl. The IIA (2004a), PA 1130-A1-2: Verantwortung des internen Audits für andere (nicht im Fachgebiet des Audit liegende) Funktionen. 10) Vgl. The IIA (2004a), PA 2100-3: Die Rolle des internen Audit im Risikomanagementprozess. 11) Vgl. The IIA (2004a), IIA-Standard 2010-A1: «Die Prüfungsplanung des Internen Audit erfolgt auf Basis einer Risikobeurteilung, die mindestens einmal pro Jahr durchzuführen ist. Der Input der Leitung der Organisation und des Überwachungsorgans werden dabei berücksichtigt.» 12) Vgl. COSO (2004a) und COSO (2004b) sowie Ruud/Sommer (2006). 13) Vgl. The IIA UK (2003). 14) Vgl. zur «Verbindung» des internen Audits und des Riskmanagements auch Beumer (2005) und zum Riskmanagement als Grundlage für die Prüfungsplanung Baeriswyl/Zehnder (2002). Auch vgl. The IIA (2004a): PA 2010-2: Verknüpfung der Prüfungsplanung mit Risiken und Risikopotentialen. 15) Vgl. Beasley/Clune/Hermanson (2005), Conference Board (2005), Walker/Shenkir/Barton (2002) und Miccoli/Hively/Merkley (2001). 16) Vgl. Beasley/Clune/Hermanson (2005),

S. 69–72 auch für die nachfolgenden Ausführungen. Befragt wurden über 1700 Mitglieder des IIA Global Auditing Information Network (GAIN). Mit einer ungefähren Rücklaufquote von 10% (175 Antworten) haben eher grosse Unternehmen (Umsatz: Median=1,3 Mrd. USD) mit durchschnittlich 14 internen Auditoren aus vorwiegend englischsprachigen Ländern (USA [68%], Kanada [10%], Grossbritannien [5%], Australien [5%] und andere [12%]) geantwortet. 17) Vgl. Conference Board (2005), o. S.

Literatur: ► Beariswyl, Stefan/Zehnder, Martina (2002): Das Risk Management als Grundlage für die Revisionsplanung der Internen Revision – Fallbeispiel Schweizerische Post, in: Der Schweizer Treuhänder, 3/2002, S. 149–154. ► Beasley, Mark S./Clune, Richard/Hermanson, Dana R. (2005): ERM a Status Report, in: Internal Auditor, February 2005, Vol. 62, Issue 1, S. 67–72. ► Beumer, Hans (2005): Linkage of Internal Audit and Risk Management – Practice at Saurer, in: Der Schweizer Treuhänder, 6–7/2005, S. 441–447. ► Bundesrat (2005): Entwurf des Obligationenrechts; Änderung vom 16. Dezember 2005 (Vorlage der Redaktionskommission für die Schlussabstimmung), Abrufbar im Internet unter: <http://www.parlament.ch/se-schlussabstimmung-01-082-1.pdf>, Stand: 9. Januar 2006. ► 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. ► Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004a): Enterprise Risk Management – Integrated Framework: Executive Summary, Framework, Jersey City (NJ), 2004. ► Committee of Sponso-

ring Organizations of the Treadway Commission (COSO) (2004b): Enterprise Risk Management – Integrated Framework: Application Techniques, Jersey City (NJ), 2004. ► Economiesuisse (2002): Swiss Code of Best Practice for Corporate Governance, Economiesuisse, 2002. ► Jackson, Russel A. (2005): Role Play, in: Internal Auditor, April 2005, Vol. 62, Issue 2, S. 44–50. ► Miccoli, Jerry A./Hively, Kevin/Merkley, Brian W. (2001): Enterprise Risk Management: Trends and Emerging Practices, The IIA Research Foundation, Altamonte Springs, 2001. ► Ruud, Flemming T./Sommer, Katerina (2006): Enterprise Risk Management – Das COSO-ERM-Framework, in: Der Schweizer Treuhänder, 3/2006, S. 126–131. ► The Institute of Internal Auditors (The IIA) (2004a): The Professional Practices Framework, Altamonte Springs (FL), 2004. Für die offizielle deutsche Übersetzung: Deutsches 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 – UK and Ireland (The IIA UK) (2003): Risk Based Internal Auditing. Abrufbar im Internet unter: <http://www.blindtiger.co.uk/IIA/uploads/48dc2e62-f2a7bd939a--7cef/RiskBasedInternalAuditing.pdf>, Stand: 5. Dezember 2005. ► Walker, Paul L/Shenkir, William G./Barton, Thomas L. (2002): Enterprise Risk Management – Pulling it All Together, The IIA Research Foundation, Altamonte Springs, 2002.

RESUME

Audit interne et gestion des risques dans l'entreprise

En matière de gestion des risques dans l'entreprise, *Enterprise Risk Management (ERM)*, la mission centrale de l'audit interne consiste à apporter son soutien au conseil d'administration et à la direction en vérifiant si les procédures de gestion des risques sont adéquates et efficaces, en les analysant, puis en rédigeant un rapport à leur sujet contenant des propositions d'améliorations. Dans le domaine de l'ERM, l'audit interne peut également avoir une fonction de conseil dont l'ampleur dépend de la disponibilité d'autres ressources, internes et externes, ainsi que de l'évolution du degré de maturité de l'entreprise en matière de gestion des risques. Lors de l'examen de la compatibilité des prestations de conseil et des prestations d'assurances, il est décisif de savoir si les auditeurs internes assument également des responsabilités de management. L'audit interne peut étendre son intégration à l'ERM à tra-

vers les prestations d'assurance, mais ceci, à condition que ne lui incombe aucune responsabilité en matière de gestion des risques et que demeurent garanties certaines mesures de protection. Lors de la définition du rôle de l'audit interne en matière d'ERM, il faut vérifier que ces activités n'entravent ni l'indépendance, ni l'objectivité de l'auditeur interne et évaluer la probabilité selon laquelle ces activités sont susceptibles de contribuer à améliorer les procédures de gestion des risques, de pilotage, de contrôle et de bonne gouvernance.

L'ERM et l'audit interne sont en interaction: d'une part, l'audit interne évalue le système de gestion des risques au sein de l'entreprise; de l'autre, les informations provenant de l'ERM peuvent constituer une base de travail pour ce même audit interne. Dans le cadre d'un concept de vérification «traditionnellement» orienté vers les risques, on se

concentre davantage sur les risques d'audit et moins sur les risques commerciaux. Si l'entreprise dispose d'une ERM, il semble logique, lors de la planification de l'audit, d'intégrer les informations issues de la procédure ERM dans l'évaluation des risques, puis dans le déroulement de la vérification (audit interne reposant sur le risque). La différence essentielle réside dans le fait que, dans le cadre d'un audit interne reposant sur le risque, l'accent est mis sur la compréhension et l'analyse de l'évaluation des risques par le management et que la procédure d'audit se fonde sur l'évaluation des risques par le management. Les résultats issus de telles vérifications peuvent être intégrés dans l'évaluation des risques telle qu'elle est prévue dans le cadre de l'ERM. Il convient de mettre à profit ces synergies potentielles, ce qui n'est aujourd'hui le cas, hélas, que dans très peu d'entreprises. TFR/KS/JA