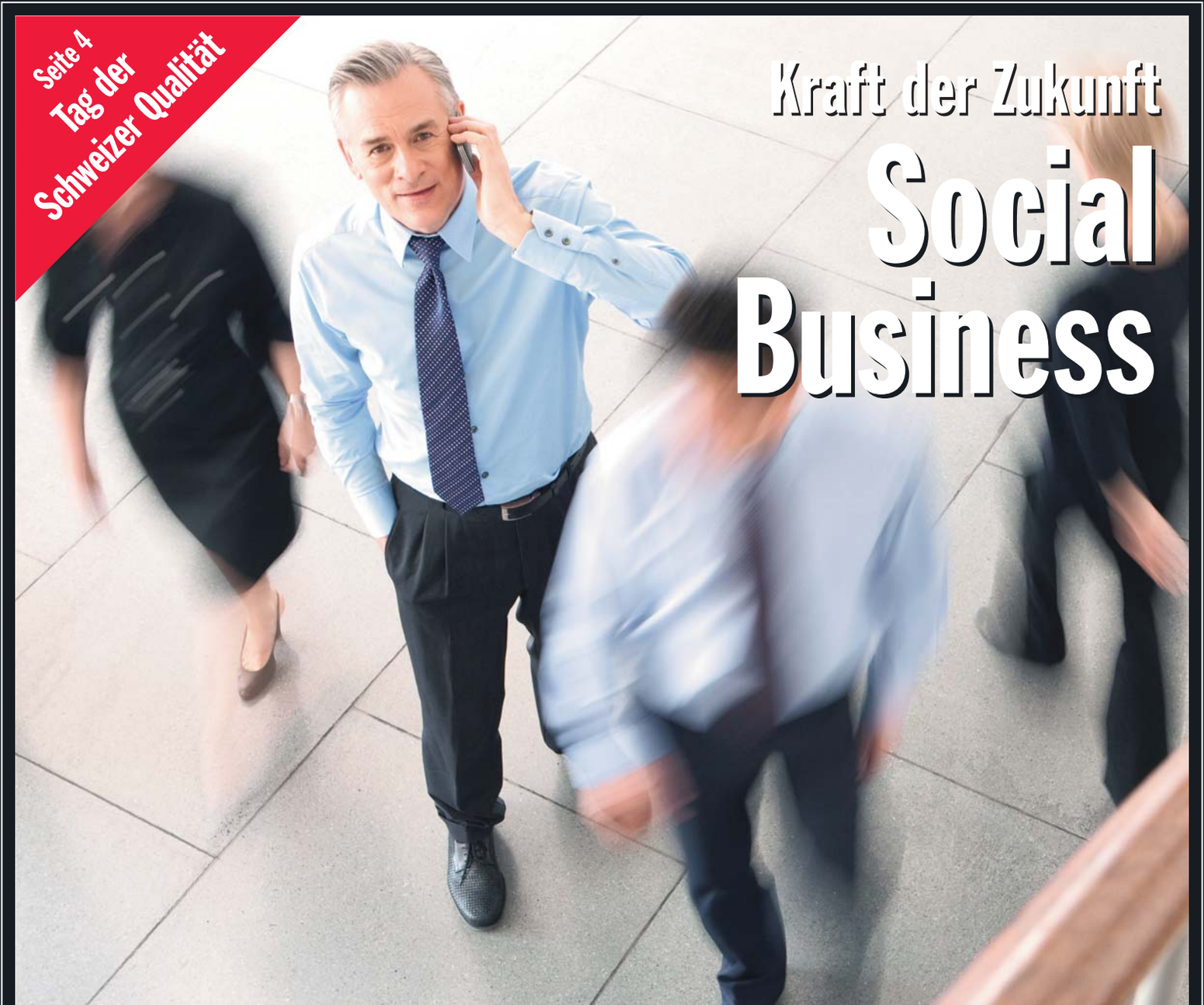
42. Jahrgang CHF 14.30

MQ Management und Qualität

Ausgabe 7-8/2012

Das Magazin für integrierte Managementsysteme



Seite 4
Tag der Schweizer Qualität

Kraft der Zukunft

Social Business

Gescheit wirtschaften

KMU und Nachhaltigkeit Seite 8

Sicherheit zuerst. Qualität auch.

IQSoft bei der Montana Bausysteme AG Seite 15

Es lebe das Web!

Das andere Wissensmanagement Seite 18

Goldfeder-manufaktur

Reorganisation der Montblanc-Fertigung Seite 30

MQ Risikomanagement: ISO 31000 auf Erfolgskurs

Risikomanagement

ISO 31000:2009 auf Erfolgskurs

Von Heinrich Kuhn

Seit 2009 ist die internationale Risikomanagement-Norm ISO 31000:2009 in Kraft. Nach drei Jahren praktischer Erfahrung mit dieser neuen Norm fand im Mai 2012 die «First International Conference on ISO 31000» in Paris statt. Sie diente der Standortbestimmung, aber auch der Entwicklung einer Roadmap für die kommenden Jahre.

Vor rund einem Jahrzehnt herrschte eine grosse Vielfalt von nationalen und internationalen Risikomanagement-Vereinigungen und deren Risikomanagement-Normen. Die Vielfalt war verwirrend und verhinderte damit letztendlich, dass sich das Risikomanagement zu einem wirkungsvollen Managementansatz entwickeln konnte. Dieser Umstand war einer der wichtigen Gründe, warum ISO im Jahr 2005 die Initiative ergriff, eine generische Leit-Norm für das Risikomanagement zu entwickeln. Im Jahr 2009 wurde diese Arbeit abgeschlossen und die ISO 31000:2009 unter dem Titel «Risk management Principles and guidelines» publiziert.

Prof. Heinrich Kuhn, Kompetenzzentrum für Sicherheits- und Risikomanagement (KSR), Zürcher Hochschule für Angewandte Wissenschaften, ZHAW, Leiter des Masters of Advanced Studies in Integrated Risk Management (MAS IRM), Mitglied SNV des TC 262: ISO 31004:2014 Risk management, Implementation Standard for ISO 31000:2009, CH-8401 Winterthur, T +41 (0)58 934 77 30, heinrich.kuhn@zhaw.ch

G31000-Konferenz

An der G31000-Konferenz, der «First International Conference on ISO 31000», nahmen rund 120 Teilnehmerinnen und Teilnehmer teil (www.G31000conference2012.org). Gut vertreten waren Europa, die USA, Kanada, Australien und Neuseeland. Es gab eine kleinere Gruppe von Teilnehmenden aus dem Umfeld der AS/NZS 4360:2004. Diese australische und neuseeländische Norm galt lange als beste nationale RM-Norm. Sie diente bei der Erarbeitung der ISO 31000:2009 als Arbeitsgrundlage, die adaptiert und auch erweitert wurde. Die Mehrzahl der Teilnehmenden gehörte aber der neuen RM-Generation, der ISO-31000-Generation, an.

Internationaler Survey

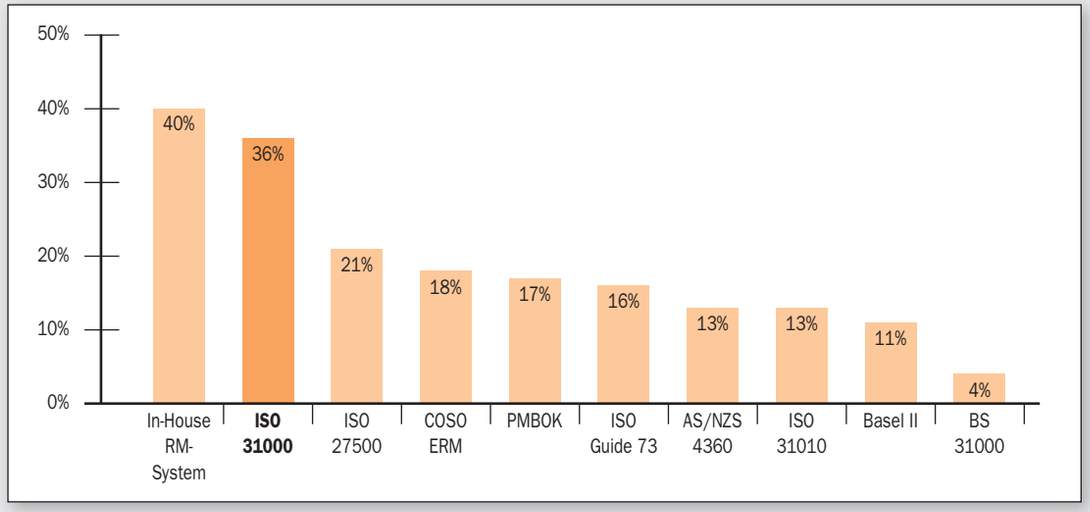
Im Vorfeld dieser Konferenz wurde in der zweiten Jahreshälfte 2011 ein «First Global ISO 31000 Survey 2011» durchgeführt. Sämtliche der rund 75 wichtigen nationalen und internationalen Risikomanagement-Vereinigungen wurden eingeladen, an diesem Survey teilzunehmen. Der Survey umfasste fünfzehn Fragen, die von 1823 Risikomanagern und Vertretern dieser RM-Vereinigungen aus insgesamt 111 Ländern beantwortet wurden. Erste Resultate dieses Surveys wurden an der Pariser Konferenz vorgestellt. Nämlich die Auswertungen zu den Fragen:

- 1. Welche Normen verwenden Sie in Ihrem Unternehmen/Ihrer Organisation?
- 2. Wofür wird in Ihrem Unternehmen/Ihrer Organisation RM verwendet?

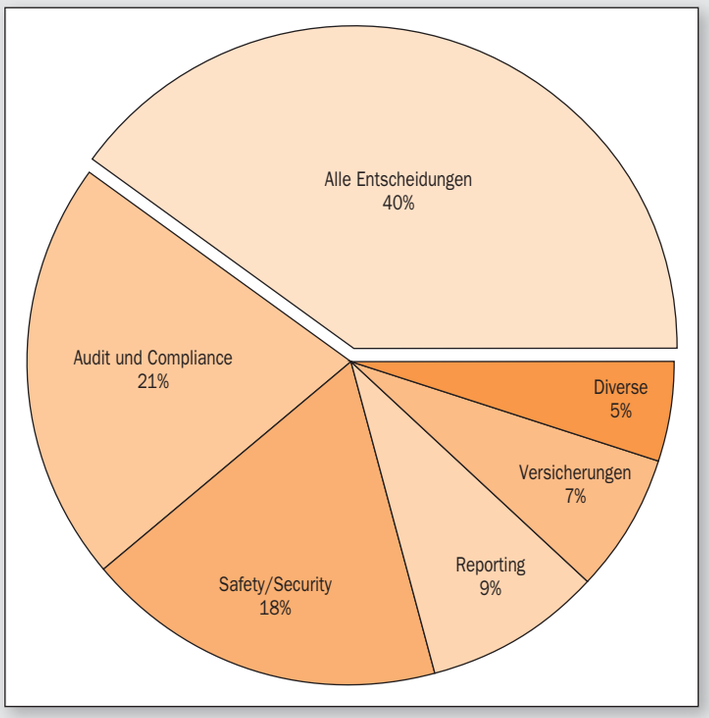
Bei der ersten Frage war es möglich, mehrere Antworten zu geben, da gerade in grösseren Unternehmen oft unterschiedliche RM-Systeme im Einsatz sind. Erstaunlich bei den Resultaten ist, dass die ISO 31000:2009 mit 36 Prozent Anteil auf dem zweiten Platz ist. Weniger erstaunlich ist, dass die sog. «In-House RM-Systems» den ersten Platz belegen (Grafik 1).

Risikomanagement existiert natürlich nicht erst seit 2009 und darum haben viele Unternehmen eine individuelle Lösung für ihre spezifische Risikoexposition entwickelt. Was auch auffällt, ist, dass bei dieser Umfrage unter den Top-10-Nennungen neben der IS0 31000:2009 auch die mit ihr assoziierten Normen ISO Guide

RM-Normen in Unternehmen Grafik 1



RM-Einsatz Grafik 2



73, ISO 31010:2010, BS 31000:2011 und die AS/NZS 4360:2004 genannt werden. Diese fünf Normen bilden einen eigentlichen ISO Cluster. Andere RM-Systeme wie Basel II (11 Prozent) und auch COSO (18 Prozent) (COSO: Committee of Sponsoring Organizations of the Treadway Commission) wurden deutlich weniger häufig genannt. Das ist insofern erstaunlich, weil etwa der COSO-Ansatz schon seit rund 20 Jahren im Einsatz ist. Der ISO-31000-Ansatz hat es also in knapp drei Jahren geschafft, den ersten Platz unter den offiziellen RM-Standards zu erlangen.

Auch die Auswertung der zweiten Frage, wofür Risikomanagement in den Unternehmen eingesetzt wird, liefert sehr interessante Ergebnisse: Die Anwendungen, in denen früher das traditionelle Risikomanagement eingesetzt wurde, nämlich vor allem Safety/Security (zum Beispiel Arbeits-, Prozess- und Produktsicherheit), versicherungstechnische und finanzielle Abschätzungen (inkl. Reporting) finden sich erst ab dem dritten Platz. Auch hier zeigt sich der Einfluss von ISO 31000:2009: Modernes Risikomanagement geht von der Voraussetzung aus, dass das RM bei allen relevanten Unternehmensentscheidungen berücksichtigt wird (Platz 1) und dass ein internes Audit sich auf die risikorelevanten Werte (Platz 2) fokussiert – und insofern auch die Compliance unterstützt. Risikomanagement ist nicht länger nur eine Frage der operationellen Risiken, sondern das moderne Risikomanagement ist im Umfeld der Geschäftsleitung und der Aufsichtsorgane angekommen. Die Auswertung der beiden Survey-Fragen zeigt, dass die ISO 31000:2009 innerhalb von nur drei Jahren für Unternehmen und Organisationen zum offiziellen Risikomanagement-Benchmark geworden ist (Grafik 2).

Was die Zukunft bringt

Neben diesen überraschenden Ergebnissen, die im Rahmen einer Standortbestimmung diskutiert wurden, stand auch die Frage im Zentrum, wie es weitergehen soll. Im Zusammenhang mit einer solchen Roadmap wurden folgende Schwerpunkte diskutiert:

- a. Implementierung der ISO 31000:2009: ISO 310004 und Maturitäts-/Reifegradmodelle
- b. Förderung des neuen Denkansatzes: Der Paradigmenwechsel im RM durch die ISO 31000:2009
- c. Integrierte Managementsysteme

Implementierung und ISO 31004:2014

Die Stärke der ISO 31000:2009, dass sie einen generischen, also übergreifenden Ansatz vertritt, ist für manche RM-Verantwortliche aber auch ein gewisses Problem. In den «Grundsätzen» (Principles) zur ISO 31000:2009 heisst es: Risikomanagement ist massgeschneidert (tailored). Darum wurde in den vergangenen drei Jahren eine Anzahl an Guidelines zur ISO 31000:2009 publiziert. Im deutschsprachigen Raum ist dies die ONR 49000-49003:2010, die diese Funktion erfüllt. In andern Ländern entstanden ähnliche nationale Guidelines (Grafik 3).

Das Interessante an diesen Dokumenten ist, dass es eine recht grosse Bandbreite gibt, wie die ISO 31000:2009 konkretisiert und auch strukturiert werden kann. Diese Vielfalt ist sehr bereichernd. Anderseits ist es natürlich aber nur bedingt ein Vorteil, wenn die internationale ISO 31000:2009 mit einer nationalen Guideline konkretisiert wird. Dies betrifft insbesondere global tätige Unternehmungen. Darum initiierte ISO die Entwicklung der ISO 31004:2014, die diese Guideline-Funktion in einem internationalen Umfeld erfüllen soll. Die Publikation wird anfangs 2014 erwartet. An der G31000-Konferenz wurde diese neue ISO-Publikation sehr begrüsst.

Praktikable Maturitätsmodelle

Die ISO 31000:2009 basiert auf einem umfassenden Corporate-Risk-Management-Modell, wie es zum Beispiel in Grossunternehmen verwendet wird. Wenn die ISO 31000:2009 in einem beschränkteren Umfang eingesetzt werden soll, ist es notwendig, dieses Modell mit einem Maturitäts- oder Reifegradmodell zu verbinden.

Ein sehr interessanter Ansatz wurde im Rahmen der kanadischen Norm Q31001-11 entwickelt. Wichtige Ausführungen finden sich auch in der britischen Norm BS 31100:2011. Selbstverständlich ist die Entwicklung von solchen Maturitätsmodellen keine Erfindung des Risikomanagements. Im Qualitätsmanagement, im IT-Security- und auch IKS-Umfeld finden sich analoge Modelle. Diese müssen dann aber in jedem Fall noch sinnvoll auf das ISO-31000-RM-Modell adaptiert werden. Auf der Grundlage solcher Guidelines wie der ISO 31004:2014 und praktikabler Maturitätsmodelle wird es für alle RM-Anwenderinnen und -Anwender sehr viel einfacher, diese Leit-Norm entsprechend den realen Rahmenbedingungen zu implementieren. So kann die ISO 31000:2009 ihren maximalen Nutzen entfalten. An der G31000-Konferenz herrschte der Konsens, dass es von zentraler Bedeutung ist, solche Maturitätsmodelle zu entwickeln und zu fördern.

Paradigmenwechsel durch die ISO 31000:2009

Traditionelles Risikomanagement ist primär auf Schäden, Fehlfunktionen, Ausfallraten und Verluste fokussiert. Im Gegensatz dazu fokussiert der Ansatz der ISO 31000:2009 primär auf die strategischen und operativen Unternehmensziele, aber auch die Leistungs- und die regulatori-

schen Ziele. Dieser Paradigmenwechsel im Risikomanagement zeigt sich sowohl in der ISO-Risikodefinition «risk is the effect … on objectives» als auch im RM-Modell der ISO 31000:2009. Die ISO-Definition berücksichtigt nicht nur unternehmensinterne Zielbereiche, sondern auch die unternehmensexternen, die sich zum Beispiel aufgrund einer Stakeholderanalyse ergeben und die für den Erfolg eines Unternehmens entscheidend sein können.

Der grosse Vorteil dieses neuen RM-Ansatzes ist, dass das Risiko- und das Chancenmanagement eine enge Verbindung eingehen: Das Risikomanagement schützt die Unternehmensziele; es fördert sie aber auch aktiv. Indem das Risikoassessment klar auf die Ziele eines Unternehmens ausgerichtet ist, ist es mit einem grösseren Objektivitätsgrad möglich, diese Risiken nachvollziehbar zu beurteilen. Wenn etwa ein strategisches Ziel durch ein gewisses Ereignis stark betroffen wird, ist es klar, dass es sich sicher nicht um ein kleines oder mittleres Risiko handeln kann. Auch wenn die Vorteile dieses neuen Denkansatzes, dieses Paradigmenwechsels, unbestritten sind, so ist doch festzustellen, dass dieser neue Denkansatz noch nicht überall umgesetzt wird. Darum wurde an der G31000-Konferenz gefordert, dass die Awareness für diesen Paradigmenwechsel aktiv gefördert werden soll, damit dieses neue Paradigma noch besser verankert und umgesetzt wird.

Neues Denken im BCM

Die ISO 31000:2009 vertritt einen integrativen Managementansatz. Darum ist es folgerichtig, dass diese ISO-Norm und das Business Continuity Management (BCM) in eine sinnvolle Verbindung gebracht werden. Im BCM-Bereich dominiert bis heute klar die BS 25999 das Unternehmensumfeld. Diese britische Norm geht davon aus, dass das BCM nicht notwendig auf einem Risikomanagement basieren muss. Entgegen diesem britischen BCM-Ansatz, der BCM und RM als unabhängige Inseln betrachtet, entstanden im australisch-neuseeländischen Umfeld drei BCM-Normen, die mit der ISO 31000:2009 voll kompatibel sind:

- HB 221:2004: Business Continuity Management
- HB 292/293:2006: Business Continuity Management Handbooks
- AS/NZS 5050:2010: Business continuity – Managing disruption-related risk

Der Vorteil dieser Normen ist, dass Risiken mit Entwicklungscharakter sowohl im Risikomanagement als auch in einem BCM-Ansatz erfasst und somit in einem integrativen Gesamtmodell abgebildet werden können. Als Beispiel dieser Kategorie könnte man den globalen Toyota-Rückruf erwähnen, der als ein Qualitätsproblem im RM-Umfeld begann – und der dann als die teuerste Rückrufaktion in den USA in die Geschichte einging. Integrative RM-BCM-Modelle haben den Vorteil, eine wichtige Frühwarnfunktion zu haben.

Die AS/NZS 5050:2010 ist insofern interessant, weil sie sich auch an den Zielen eines Unternehmens orientiert. In Bezug auf ihren methodischen Ansatz ist sie das logische Pendant zur ISO 31000:2009. An der G31000-Konferenz wurden diese neuen Modelle einer integrativen Sichtweise sehr angeregt diskutiert.

Integrierte Managementsysteme als Erfolgsmodell

Die Konferenz hatte in Bezug auf das Thema RM – BCM den Charakter eines Think Tanks, in dem neue BCM-Normen und deren Integration diskutiert wurden, in der Erwartung, leistungsfähigere BCM-Instrumente entwickeln zu können. Eine wirklich sehr interessante Diskussion!

In Bezug auf die Integration des Risikomanagements nach ISO 31000:2009 in einen übergreifenden Managementsystem-Ansatz herrschte an der Konferenz ein klarer Konsens: Durch die Integration des Risikomanagements in bestehende Managementsysteme wird die Bedeutung des Risikomanagements klar gestärkt.

Die alte Variante, das Risikomanagement als eine «Insel» im Unternehmen zu führen, hat dem gegenüber keine Zukunft. Darum ist zu erwarten, dass die heute noch verbreiteten «In-House RM-Systems» deutlich an Bedeutung verlieren werden, respektive durch ISO-31000-kompatible Lösungen ersetzt werden.

Fazit

Zusammenfassend kann man festhalten, dass die RM-Leitnorm ISO 31000:2009 sich innerhalb von rund drei Jahren klar als Benchmark global durchgesetzt hat. Die nächste Konferenz zur ISO 31000:2009 findet im Frühling 2013 in Toronto statt. Man darf gespannt sein, wie die Entwicklung weitergeht und welche neuen Erkenntnisse nächstes Jahr in der Konferenz-Agenda stehen werden. ■

Normen und Guidelines

Grafik 3

Typ	Bezeichnung	Titel	Region
RM-Norm	AS/NZS 4360:2004	Risk management	Australien, Neuseeland, Commonwealth (z.T.)
ISO-Norm	ISO 31000:2009	Risk management – Principles and guidelines	global
	ISO 31010:2009	Risk management – Risk assessment techniques	global
	Guide 73:2009	Risk management – Vocabulary	global
Guideline national	JIS Q 2001:2001:2007	Guidelines for development and implementation of risk management system	Japan
	ONR 49000-49003:2010	Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen – Umsetzung von ISO 31000 in die Praxis	Österreich, Schweiz (SAQ), Deutschland (TÜV)
	NWA 31000:2010	National Guidance on implementing I.S. ISO 31000:2009 Risk management – Principles and Guidelines	Irland
	BS 31100:2011	Risk management. Code of practice and guidance for the implementation of BS ISO 31000	Grossbritannien
	Q31001-11	Implementation guide to CAN/CSA-ISO 31000, Risk management – Principles and guidelines	Kanada
Guideline global	ISO 31004:2014	Guidance for the implementation of ISO 31000	global