Brühwiler Bruno

Risikomanagement für Organisationen und Systeme

Die neue normative Grundlage ONR 49000 ff

Die Entwicklung des Risikomanagements ist dadurch gekennzeichnet, dass sich seine Anwendung ursprünglich nur auf „Safety & Security“ erstreckte. Erst in jüngster Zeit befasst sich das Risikomanagement in umfassender Weise mit den Risiken von Organisationen (private, öffentliche, gemeinnützige), Produkten, Dienstleistungen oder Projekten. In diesem Zusammenhang ist es zweckmäßig, den Risikobegriff zu öffnen und ihn als Inbegriff von Chance und Gefahr zu verstehen.

Die neuen ON-Regelungen Risikomanagement für Organisationen und Systeme sollen mit einem umfassenden Ansatz den Managern im Umgang mit Risiken helfen. Allerdings soll durch zusätzliche Normung nicht die Kostenspirale angetrieben werden. Vielmehr zielt das Risikomanagement auf die Verbeserung der Wertschöpfung ab.

EINLEITUNG

NORMATIVE GRUNDLAGEN IM RISIKOMANAGEMENT

Die erste normative Grundlage zum Risikomanagement ist der US-MIL-STD 882, eine Vorgabe des US-Verteidigungsministeriums für die Analyse von Risiken technischer Systeme. Sie wurde in den Siebziger Jahren von der damaligen Zürich Versicherung zur „Zurich Hazard Analysis“ weiterentwickelt. Inzwischen sind zum Thema Risikomanagement bedeutende normative Grundlagen entstanden. Hier ein Auszug:

- ISO Guide 51 (DIN 820-120:2001-10) (D): *Leitfaden für die Aufnahme von Sicherheitsaspekten in die Normung.*
- ISO Guide 73:2002 (F/E): *Risk Management – Vocabulary – Guidelines for use in standards*
- ISO 14121 (EN 1050): *Sicherheit von Maschinen – Leitfaden zur Risikobeurteilung*
- ISO 14971:2000: *Medizinprodukte – Anwendung des Risikom. auf Medizinprodukte*
- ISO FDIS 17666: *Space Systems – Risk Management*
- EN ISO 17776:2000: *Erdöl- und Erdgasindustrie – Offshore Produktionsanlagen – Leitfaden zur Gefahrenerkennung und Risikobeurteilung*

Zu diesen Dokumenten kommen mehrere Normen für Methoden der Risikoanalyse hinzu, etwa die FMEA (DIN IEC 60812), die in der Automobil-Industrie weit verbreitet ist, die Methoden der Störungsbaum-Analyse (DIN IEC 1025, DIN 25424) und Ereignisablaufanalyse (DIN 25419). Methoden der Risikoanalyse sind wichtige Elemente des Risikomanagements, aber nicht die einzigen.

Eine Eigenheit der oben aufgeführten normativen Grundlagen besteht darin, dass sie sich in der Regel mit Sicherheitsfragen von technischen Systemen auseinander setzen. Die Sicherheit von Personen, Sachen und der Umwelt steht im Mittelpunkt. Wir bewegen uns im Bereich des Sicherheitsmanagements.

Mitte der Neunziger Jahre entstand der Australisch-Neuseeländische Risk Management-Standard, der AS/NZS 4360: 1999 Risk Management. Im Gegensatz zu eher technisch ausgerichteten Regelwerken beabsichtigt diese Norm, das Risikomanagement in Organisationen hineinzutragen. Dieser RM-Standard ist vor allem im südostasiatischen Raum (einschliesslich Japan) verbreitet.

GESETZE UND INTERNATIONALE VEREINBARUNGEN

Inzwischen hat Risikomanagement weitere Kreise gezogen. Gesetze verlangen Risikomanagement, so etwa in Deutschland das KonTraG von 1998 (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, es verpflichtete den Vorstand einer Deutschen Aktiengesellschaft eine Überwachungssystem einzuführen) oder in den USA der Sarbanes-Oxley Act von 2002. Bei ihm geht es um die interne und externe Kontrolle der finanziellen Berichterstattung von börsennotierten Unternehmen. Das Risikomanagement soll dabei nach dem „Enterprise Risk Management Framework COSO“ (Committee of Sponsoring Organization of the Treadway) erfolgen.

Von erheblicher Bedeutung für die europäische Finanzwirtschaft dürften die Internationalen Konzepte von BASEL II (Banken) und SOLVENCY II (Versicherungen) in der Finanzindustrie sein. Sie verlangen explizit die Berücksichtigung aller Risiken in der Eigenmittelausstattung.

Damit sind die vielfältigen Anforderungen an einen Risikomanagement-Standard aufgezeigt. Risikomanagement muss heute ein umfassender Ansatz sein. Die neuen ON-Regeln Risikomanagement für Organisationen und Systeme (ONR-49000 ff.) erfüllen diese Anforderungen. Sie wollen aber den Unternehmen und Organisationen keinesfalls neue Vorschriften auferlegen, wie es in den USA mit Sarbanes-Oxley gegenwärtig geschieht. Die neuen ONRs verstehen sich

als Hilfestellung für Manager, die wissen wollen, wie sie am besten mit ihren Risiken umgehen können.

DAS NEUE REGELWERK RISIKOMANAGEMENT ONR-49000 FF.

BREITE TRÄGERSCHAFT

Zwei Arbeitsgruppen, die Fachgruppe „Risikomanagement“ der Swiss Association for Quality (SAQ) sowie der Arbeitskreis „Risikomanagement“ des Österreichischen Normungsinstituts (ON) haben sich zur Aufgabe gemacht, ein Regelwerk zum Thema Risikomanagement zu verfassen, um in das schwierige und komplexe Thema Übersicht und Ordnung hineinzubringen. Das Regelwerk ist zwar (noch) keine Norm, dürfte sich aber in diese Richtung entwickeln.

Das Regelwerk Risikomanagement wird von namhaften Unternehmen mehrerer Wirtschaftszweige aus der Schweiz, aus Österreich und Deutschland getragen, auch von international tätigen Versicherern, die schon längst im Kerngeschäft der Industrieversicherung Risikomanagement betreiben. Auch namhafte Wissenschafter und Beratungsunternehmen aus Österreich, Deutschland und der Schweiz haben die Entstehung des Regelwerkes begleitet. Die Ursprungsrechte liegen beim Österreichischen Normungsinstitut in Wien.

ZIEL UND ZWECK

Das Regelwerk Risikomanagement soll – aufbauend auf vorhandenen normativen Grundlagen - einen übergeordneten, offenen und umfassenden Rahmen für das Risikomanagement von Organisationen und Systemen schaffen. Durch die Anpassung an die individuellen Gegebenheiten und Bedürfnisse kann das Risikomanagement in unterschiedlichen Gebieten, aber auf einheitlichen Grundlagen, Begriffen, Methoden und System-Elementen angewendet werden.

STRUKTUR DES REGELWERKES RISIKOMANAGEMENT

Das neue Regelwerk zum Risikomanagement umfasst mehrere Teile. Am Anfang stehen – wie auch bei anderen Regelwerken und Normen - die „Begriffe und Grundlagen“. Es werden sodann die „Elemente des Risikomanagement-Systems“ beschrieben. Der „Leitfaden für das Risikomanagement“ sowie der „Leitfaden für die Einbettung des Risikomanagements ins Managementsystem“ zeigen auf, wie man die Elemente des Risikomanagement-Systems in der Praxis umsetzen kann. Den Abschluss bilden die „Anforderungen an die Ausbildung des Risikomanagers“.

Das Regelwerk beschreibt das Risikomanagement-System dergestalt, dass es möglich ist, aufgrund der festgelegten Anforderungen zu überprüfen, ob die grundlegenden Elemente des Risikomanagement-Systems vorhanden und im Management-System funktionstüchtig integriert sind. Mit dem Regelwerk schaffen wir auch die Möglichkeit, die Ausbildung des Risikomanagers zertifizieren zu lassen.

DAS RISIKOMANAGEMENT KONZEPT

RISIKOMANAGEMENT IM KONTEXT DER ORGANISATION

Die Risikobeurteilung und das Risikomanagement stehen im Kontext, der durch die Systemabgrenzung gegeben ist.

In vielen Fällen ist die Organisation der Rahmen, in dem die Risikopolitik und das Risikomanagement stattfinden. Sie verfolgt Ziele und steht in einem Umfeld, das Anforderungen und Erwartungen an sie stellt. Die Ziele lassen sich inhaltlich in verschiedene Bereiche gliedern, wofür es z.B. Unternehmens-Modelle gibt wie Balanced Scorecards. Analog gibt es Risiken, die Kunden / Produkte, operative Prozesse, Finanzen oder Fähigkeiten der Organisation betreffen.

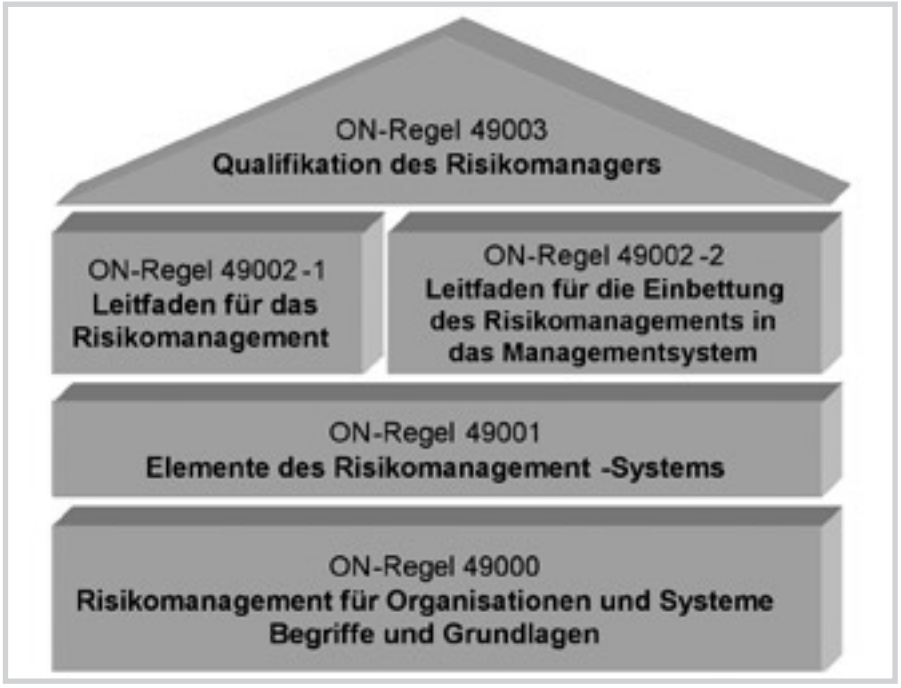

Abb. 1: Aufbau der ONR-Gruppe 49000 ff.

Das Umfeld einer Organisation, aus dem die Erwartungen entstehen, wird oft unterteilt in Gesellschaft-Recht-Politik, Wirtschaft, Technik-Sicherheit und Umwelt-Ökologie. Risiken stellen dann Bedrohungen der Ziele oder eine fehlende Übereinstimmung der Organisation mit den Erwartungen aus dem Umfeld dar. Die Risikopolitik formuliert die Inhalte und die Art der Durchführung des Risikomanagements.

Die Risikopolitik einer Organisation beinhaltet die Ziele, Strategien und Ressourcen für den Umgang mit Risiken. Das Risikomanagement umfasst die Systemdefinition, die Risikobeurteilung, die Risikobewältigung und die Risikoüberwachung.

Das neue Regelwerk Risikomanagement baut auf einem umfassenden Risikoverständnis auf und strebt eine Gesamtsicht der Risiken eines betrachteten Systems bzw. einer Organisation an. Somit geht das neue Regelwerk weit über das traditionelle Sicherheitsmanagement hinaus.

RISIKOMANAGEMENT

Das Ursprungskonzept des Risikomanagements konzentriert sich auf mehrere Schritte oder Phasen, die sich z.B. mit den vier Begriffen

> „Systemdefinition“,
> „Risikobeurteilung“,
> „Risikobewältigung“ und
> „Risikoüberwachung“

darstellen lassen.

Die Besonderheit des Risikomanagements als Führungstätigkeit liegt in den Inhalten dieser vier Schritte. Nachfolgend sollen sie kurz erörtert werden.

Systemdefinition

Eine Risikobeurteilung erfordert zuerst, dass ihr Ziel und Zweck festgelegt wird (wozu dient die Risikobeurteilung). Auch der organisatorische Rahmen muss definiert sein (die Analyse-Einheit, Risikoeigner, Risikomanager). Schliesslich geht es darum, die zu berücksichtigenden Inhalte der Risikobeurteilung (welche Arten von Gefahren sind Gegenstand der Risikobeurteilung?) vorzunehmen und die Kategorien der Wahrscheinlichkeit bzw. der Auswirkungen von Risiken festzulegen.

Risikobeurteilung

Die Risikobeurteilung umfasst die Risikoanalyse (Risikoerkennung und Risikoeinschätzung nach Wahrscheinlichkeit und Auswirkung) und die Risikobewertung. Bei letzterer ist die Frage zu beantworten, ob ein eingeschätztes Risiko tragbar ist (Risikoakzeptanz = Entscheid, ein Risiko zu tragen). Die Risikobeurteilung umfasst einige Spezialitäten wie das Finden von sich gegenseitig verstärkenden Risiken, Risiken die durch eine Maßnahme gegenläufig verändert werden oder Regeln für die Rechtfertigung eines Restrisikos, das immer noch über der festgelegten Risikotoleranzgrenze liegt.

Risikobewältigung

Die Risikobewältigung erfolgt nach dem „Drei-Stufen-Prinzip“. Danach müssen Risiken mit erster Priorität „konstruktiv“ beseitigt werden. Bei einem Produkt heißt dies durch Reengineering, bei

Abb. 2: Ausgangslage für das Risikomanagement

rm-norm

einer Organisation bedeutet dies eine entsprechende Änderung von Strategie oder Führung. Sind die Maßnahmen der Risikovermeidung ausgeschöpft, müssen die Restrisiken durch Maßnahmen der Risikominderung herabgesetzt werden, die die Eintrittswahrscheinlichkeit und / oder die Auswirkung verringern. Sollten immer noch nicht tragbare Restrisiken vorhanden sein, sind sie durch Information, Ausbildung, Gebrauchsanweisung, Warnung und Instruktion zu reduzieren. Für Risiken, die Folge eines plötzlich eintretenden „Ereignisses" sind, ist eine Notfallplanung erforderlich.

Risikoüberwachung

Die Risikoüberwachung erstreckt sich einerseits auf die planmäßige Durchführung der Maßnahmen der Risikobewältigung. Andererseits geht es um die Überwachung der in der Risikobeurteilung definierten Frühwarnindikatoren für Risiken, die Folge einer schleichenden Entwicklung sind.

In der ON-Regel 49002-1 Risikomanagement für Organisationen und Systeme, Leitfaden für das Risikomanagement sind diese vier Schritte des Risikomanagement-Prozesses mit einem hohen Detaillierungsgrad umfassend dargestellt.

RISIKOMANAGEMENT-SYSTEM

Aus der Politik der Organisation leitet sich die Risikopolitik ab, die von der obersten Leitung geplant, umgesetzt, überwacht und ständig verbessert wird. Damit übersteigt das Risikomanagement die Spezialistenebene. Risikomanagement wird zur Aufgabe der Führung. Dass dabei die Managementsysteme der ISO-Welt (ISO 9000 ff.) besonders hilfreich sind, mag wohl nicht erstaunen.

Viele Unternehmen haben in den vergangenen Jahren ein Managementsystem eingeführt. Weltweit nimmt das Managementsystem der ISO-9000 Familie mit rund 600.000-facher Umsetzung eine Spitzenstellung ein. Es ist deshalb von Bedeutung, dass das Risikomanagement möglichst nahtlos und damit kostengünstig in dieses Managementsystem, falls vorhanden, eingeordnet werden kann.

Ausgangspunkt bildet das dort verankerte Unternehmensmodell, das sich im Spannungsfeld zwischen Kundenbedürfnissen und Kundenzufriedenheit sowie den Anforderungen der interessierten Parteien (Shareholder und Stakeholder) bewegt. Der Führungsprozess umschließt auch das Risikomanagement.

Der gesamte Kontext zwischen der Führungstätigkeit und dem Risikomanagement kann durch seine Anbindung an den Prozess „PLAN-DO-CHECK-ACT" erfolgen. Daraus ergibt sich die Darstellung, aus der die Anforderungen bzw. die überprüfbaren Elemente des Risikomanagement-Systems als Teil eines integrierten Management-Systems abgeleitet werden können.

Ein überprüfbares Risikomanagementsystem baut auf folgenden Elementen auf:

- Allgemein: die Organisation führt das Risikomanagement-System ein, dokumentiert, hält es aufrecht und verbessert seine Wirksamkeit ständig.
- Die oberste Leitung stimmt das Risikomanagement-System mit den Zielen und Strategien der Organisation ab, legt die Risikopolitik fest, stellt die Ressourcen bereit, plant und lenkt die (interne und externe) Risikokommunikation.
- Die Risikopolitik erstreckt sich auf die für das Überleben wichtigen Risiken, berücksichtigt die Interessen der Kunden und der Stakeholder, zeigt die Faktoren auf, die Erfolg und Erfolgspotenziale bedrohen, legt die Methoden der Risikobeurteilung in verschiedenen Anwendungsgebieten

Abb. 3: Einbettung des Risikomanagements in das Qualitätsmanagement

Abb. 4: Elemente des Risikomanagement-Systems

fest, quantifiziert das Gesamtrisikopotenzial, verpflichtet sich zur Erfüllung der gestellten Anforderungen, der ständigen Verbesserung und der Überwachung der Angemessenheit des Risikomanagement-Systems.

- Das Management von Ressourcen ermittelt die Fähigkeiten der im Risikomanagement tätigen Mitarbeiter und stellt die Schulung sicher.
- Die Durchführung des Risikomanagements umfasst die Schritte Systemdefinition, Risikobeurteilung, Risikobewältigung und Risikoüberwachung.
- Risikobeurteilungen werden dokumentiert und die Fortschritte bei der Umsetzung von Massnahmen der Risikoverbesserung aufgezeichnet.
- Die oberste Leitung überwacht das Risikomanagement-System durch interne Audits und hält die Ergebnisse schriftlich fest.
- Sie verbessert die Wirksamkeit des Risikomanagement-Systems, indem die Organisation Korrektur- und Vorbeugemaßnahmen ergreift, um ungenügende Leistungen des Risikomanagement-Systems zu identifizieren und zu beheben.

Eine Organisation, die nach den Anforderungen eines solchen Risikomanagement-Systems lebt, ist in der Lage, seine Risiken zu bewältigen. Allerdings gibt es keine absolute Sicherheit, vor allem nicht gegenüber Risiken, die bisher unbekannt waren und völlig neu auftreten.

SCHNITTSTELLEN ZU ANDEREN ELEMENTEN DES MANAGEMENT-SYSTEMS

Risikomanagement hat viele Schnittstellen zu anderen Elementen des Managementsystems. Festzuhalten ist dabei, dass Risikomanagement nicht ein weiteres Teilsystem wie Qualitätsmanagement (QM), Umweltmanagement (UM) oder Sicherheitsmanagement (OSH-Occupational Safety at Health) etc. darstellt, sondern eine Querschnittfunktion mit Berührungspunkten zu allen anderen Teilsystemen ist. Die neuesten gesetzlichen Entwicklungen und internationalen Vereinbarungen dürften sogar dazu führen, dass Risikomanagement ein sehr wichtiger Teil des Managementsystems überhaupt wird. Grafisch lässt sich das Risikomanagement in ein integriertes Managementsystem einordnen.

BESONDERHEITEN DES REGELWERKES

Der Arbeitskreis Risikomanagement des Österreichischen Normungsinstituts und die Fachgruppe Risikomanagement der Swiss Association for Quality hatten sich mit dem Ziel, einen übergeordneten, offenen und umfassenden Rahmen für das Risikomanagement von Organisationen und Systemen zu schaffen, einer großen Herausforderung gestellt. Anhand einiger Hauptmerkmale des neuen Regelwerkes können signifikante Unterschiede zu anderen normativen Grundlagen am besten herausgeschält werden:

- **Vielseitige Anwendung**
  Organisationen (privat- und öffentlich-rechtliche, auch non-profit-Organisationen) und Systeme (technische Systeme, Prozesse, Projekte etc.)
- **Methoden der Risikobeurteilung**
  Risikoportfolio, dargestellt in der Risikolandschaft, Schnittstellen zu anderen Methoden der Risikoanalyse wie FMEA, Fehlerbaum- und Auswirkungsanalyse sind beschrieben
- **Differenzierte Risikobeurteilung**
  - Anpassung der Maßgrößen für die Risikobeurteilung an die Bedürfnisse der Organisation oder an das System, je nach Gegebenheiten
  - Priorisierung der Risiken einer Organisation oder eines Systems in zwei oder mehrere Risiko-Toleranzbereiche / Risiko-Toleranzgrenzen
  - Güterabwägung bei der Risiko-Nutzen-Analyse, wenn Risiko-Toleranzgrenzen aus praktischen Gründen nicht eingehalten werden können
  - Ermittlung von und Umgang mit Risiken, die in gegenseitiger Abhängigkeit stehen
  - Optimierung des Risikoportfolios bei Maßnahmen mit gegenläufiger Wirkung auf verschiedene Risiken
- **Einbindung des Risikomanagements in das Führungssystem**
  Einbindung in ein integriertes Managementsystem, u.a. durch Schaffung von Wechselbeziehungen zwischen Kernprozessen und Risikomanagement
- **Eigenständiges Risikomanagement**
  Kleinere und mittlere Unternehmen verfügen oft nicht über ein formalisiertes Managementsystem. Das Risikomanagement-System kann in einfachen Verhältnissen die Rolle des Managementsystems übernehmen

Abb. 5: Querschnittsfunktion Risikomanagement im integrierten Management-System

rm-norm

- **Wertorientierung**
  Quantitative Interpretation des Risikoportfolios mit Ableitung von Eigenkapitalerfordernissen und Angaben zum Unternehmenswert. Damit ist die normative Grundlage auch mit dem PS 340, dem Standard der Wirtschaftsprüfung für die Erfüllung der KonTraG-Anforderungen in Deutschland vereinbar
- **Ausbildung konkretisiert**
  Ausbildung und Qualifikation des Risikomanagers
- **Anerkennung möglich, aber freiwillig**
  Das Risikomanagement-System kann auf freiwilliger Grundlage anerkannt werden. Der qualifizierte Risikomanager kann auf freiwilliger Grundlage zertifiziert werden.

SCHLUSSFOLGERUNGEN

Ein Regelwerk ist eine normative Grundlage, die sich, wenn sie über entsprechende Anerkennung verfügt, rasch zur Norm auf nationaler, regionaler oder internationaler Ebene entwickeln kann. Die ONR 49000 ff. hat eine gute Voraussetzung, denn sie ist bereits sehr breit im deutschsprachigen Raum und in verschiedenen Wirtschaftszweigen abgestützt. Ihr offener und umfassender Rahmen schafft interessante Voraussetzungen für eine noch breitere Anerkennung.

Viele Organisationen zeigen gegenüber Normen einen Abwehrreflex. Es besteht die Befürchtung, dass Normen teure Zertifizierungen zur Folge haben und dadurch die Kostenspirale antreiben. Das muss nicht sein.

Eine defensive Sichtweise würde die Tatsache verkennen, dass freiwillige Normen in erster Linie helfen sollen. Sie führen zu einer Vereinfachung in der Kommunikation. Gerade im Risikomanagement ist heute in der Terminologie, den Methoden und Konzepten eine „babylonische Sprachverwirrung“ zu beobachten. Sprachbarrieren erschweren die Zusammenarbeit zwischen verschiedenen Fakultäten (Technik, Betriebswirtschaft, Finanzen, Wirtschaftsprüfung) und zwischen einzelnen Personen innerhalb der selben Fakultät. Diese zu durchbrechen und die Arbeit zu vereinfachen ist auch ein Anliegen des neuen Regelwerkes Risikomanagement.

Aber natürlich geht es bei einer normativen Grundlage für das Risikomanagement um mehr als nur um einen gemeinsamen terminologischen, methodischen und konzeptionellen Nenner. Wichtig ist, dass Organisationen in der Lage sind, Risiken zu erkennen und sie zu bewältigen. Selbst wenn nicht alle Risiken lückenlos und rechtzeitig erkannt werden können (es gibt auch immer wieder neue, bisher unbekannte Risiken), kann ein umfassendes Risikomanagement negativ einwirkende Ereignisse und Entwicklungen weitgehend verhindern und damit für das Überleben und den Wohlstand von Organisationen sehr wichtig sein.

Das Risikomanagement leistet mit bescheidenem Aufwand einen großen Beitrag zur Wertschöpfung!

Quellenhinweise:

- Österreichisches Normungsinstitut, Heinestrasse 38, 1021 Wien (www.on-norm.at):
- ONR-49000 Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen, Wien 1.1.2004
- ONR-49001 Risikomanagement für Organisationen und Systeme – Elemente des Risiko- management-Systems, Wien 1.1.2004
- ONR-49002-1 Risikomanagement für Organisationen und Systeme – Leitfaden für das Risikomanagement, Wien 1.1.2004
- ONR-49002-2 Risikomanagement für Organisationen und Systeme – Leidfaden für die Einbettung des Risikomanagements in das Managementsystem, Wien 1.1.2004
- ONR-49003 Anforderungen an die Qualifikation des Risikomanagers, Wien 1.1.2004