# Inhaltsverzeichnis

# Übersichtenverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| AKW | Atomkraftwerk |
| AIA | Automatischer Informations-Ausgleich |
| ALARP | As low as reasonably practicable |
| AS/NZS | Australian/New Zealand |
| ATC | Air Traffic Control |
| ATIR | Air Traffic Incident Report |
| ATM | Air Traffic Management |
| BAV | Bundesamt für Verkehr (Schweiz) |
| BCM | Business Continuity Management |
| BMI | Bundesministerium des Innern (Deutschland) |
| BSI | British Standard Institute |
| CAPM | Capital Asset Pricing Model |
| CEN | European Committee for Standardization / Comité Européen de Normalisation |
| CENELEC | Comité Européen de Normalisation Electrotechnique / European Committee for Electrotechnical Standardization |
| CGMPS | Current Good Manufacturing Practices |
| CIRS | Critical Incidents Reporting System |
| CobiT | Control Objectives Information Technology |
| COSO | Committee of Sponsoring Organizations of the Teeadway Commission |
| CSR | Corporate Social Responsibility |
| DIIR | Deutsches Institut für Interne Revision |
| DIN | Deutsches Institut für Normung |
| DoD | Department of Defence (USA) |
| EBIT | Earnings Before Interest and Tax |
| EFQM | European Foundation for Quality Management |
| EG | Europäische Gemeinschaft |
| EN | Europäische Norm |
| EU | Europäische Union |
| EWG | Europäische Wirtschaftsgemeinschaft |
| ERM | Enterprise Risk Management |
| F.A.Z. | Frankfurter Allgemeine Zeitung |
| FERMA | Federation of European Risk Management Associations |
| FMEA | Failure Mode and Effects Analysis / Fehler-Möglichkeiten und Einfluss-Analyse |
| GRS | Gesellschaft für Reaktorsicherheit |
| GRC | Governance, Risk and Compliance |
| HSE | Health, Safety and Environment |

| | |
|---|---|
| IEC | International Electrotechnical Commission |
| ISACA | Information Systems Audit and Control Association |
| ISO | International Standard Organization |
| ITIL | Information Technology Infrastructure Library |
| KonTraG | Deutsches Gesetz über die Kontrolle und Transparenz im Unternehmensbereich vom 30. April 1998 |
| MAS | Master of Advanced Studies (Hochschulabschluss) |
| MIL-STD | Military Standard |
| NHS | National Health Service (UK) |
| NPA | Non Prosecution Agreement (Schweizer Banken) |
| NZZ | Neue Zürcher Zeitung |
| OEM | Original Equipment Manufacturer |
| ON | Österreichisches Normungsinstitut |
| ONR | Regelwerk des Österreichischen Normungsinstituts (ON) |
| OR | Schweizerisches Obligationenrecht |
| Q | Quality |
| QRM | Qualitäts- und Risikomanagement |
| REACH | Registration, Evaluation, Authorization of Chemicals |
| RLCG | Richtlinie Corporate Governance (Schweiz) |
| RPZ | Risikoprioritätszahl |
| PRA | Probabilistic Risk Assessment |
| PrSG | Produktsicherheits-Gesetz (Schweiz) vom 1. Juli 2010 |
| PSA | Persönliche Schutzausrüstung |
| SA | Social Accountablity |
| SE | Systems Engineering |
| SEC | Securities Exchange Commission |
| SNV | Schweizerische Normenvereinigung |
| SOP | Start of Production / Standard Operation Procedure |
| SOX | Sarbanes-Oxley Act (USA) |
| STEG | Bundesgesetz über die Sicherheit von technischen Einrichtungen und Geräten |
| STEV | Verordnung über die Sicherheit von technischen Einrichtungen und Geräten |
| StGB | Schweizerisches Strafgesetzbuch |
| SUVA | Schweizerische Unfallversicherungs-Anstalt |
| UN | United Nations |
| UNCED | UN Commission on Environment and Development |
| USV | Unterbrechungsfreie Stromversorgung |
| UVEK | Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (Schweiz) |
| VaR | Value at Risk |
| VSZV | Verordnung über die Sicherheitsuntersuchung von Zwischenfällen im Verkehrswesen (VSZV) vom 17. Dezember 2014 (Stand am 1. Februar 2015) |
| WEF | World Economic Forum |

# Vorwort

Seit der Veröffentlichung der 3. Auflage dieses Buches sind fünf Jahre vergangen. Seinerzeit dominierte die Finanzkrise die Diskussionen im Risikomanagement. Warum war diese trotz der umfangreichen regulatorischen Vorgaben im Risikomanagement möglich? Die aufwendigen internen Kontrollsysteme waren offenbar nicht ausreichend wirksam, um dieses weltweite Desaster zu verhindern.

Im März 2011 ereignete sich die Nuklearkatastrophe von Fukushima. Ausgerechnet im führenden Technologieland Japan, wo zudem weltweit die größte Erfahrung mit Erdbeben und Tsunamis vorhanden ist, hat die Katastrophe stattgefunden. Wenn man Fukushima eingehend analysiert, hat die Technik trotz des Erdbebens funktioniert. Aber ein überflutetes Kernkraftwerk kann seine Funktion nicht mehr wahrnehmen. Frühere Fehlentscheidungen betreffend die Wahl des Standortes sowie die Missachtung von Sicherheitsempfehlungen der IAEA betreffend Naturkatastrophen und Tsunamis führten zum verhängnisvollen Verlauf.

Im Januar 2012 lief die Costa Concordia in Giglio / Italien auf Grund. 100 Jahre nach der Titanic spielte wenigstens das Glück mit, indem das havarierte Schiff an die Küstennähe getrieben wurde und dort liegen blieb. Unvorstellbar wären die Folgen gewesen, wenn das Schiff mit 4200 Menschen an Bord nachts auf offenem Meer gesunken wäre. Der Kapitän hat schwere Fehler begangen. Ende Juli 2012 hat die Reederei das Arbeitsverhältnis mit Schettino gekündigt. Sie hat sich von ihm öffentlich distanziert. Die Kreuzfahrtgesellschaft einigte sich im April 2013 mit der italienischen Justiz auf einen strafrechtlichen Vergleich; gegen die Zahlung von einer Million Euro – die Höchstsumme im italienischen Recht – wurden die Ermittlungen gegen das Unternehmen eingestellt. Nach Abschluss des Vergleichs wurde die Reederei auf ihr Verlangen im Prozess gegen ihren Kapitän als Nebenklägerin zugelassen. Schettino wurde am 11. Februar 2015 erstinstanzlich zu 16 Jahren und einem Monat Freiheitsstrafe verurteilt. Dieses Gerichtverfahren hat allerdings mit Risikomanagement nichts mehr zu tun.

Am 15. November 2009 wurde der Internationale Standard ISO 31000 Risk management – Principles and guidelines veröffentlicht. Es wäre vermessen zu behaupten, dass dieser globale Ansatz die vergangenen Krisen und Katastrophen hätte verhindern können. Aber die Tatsache, dass eine solche globale Norm entstanden ist, weist auf die großen Erwartungen an das Risikomanagement hin.

Inzwischen darf ich als Vorsitzender der Arbeitsgruppe ISO TC 262 WG «Core risk management standards» die Weiterentwicklung der ISO 31000 auf globaler Ebene leiten. Eine anspruchsvolle und herausfordernde Aufgabe. Auch die ONR 49000-Serie wurde inzwischen überarbeitet. Mit der Version 2014 entstand ein Regelwerk, das insbesondere in Europa hohe Anerkennung errungen hat.

Inzwischen konnte ich rund 400 Risikomanagement-Projekte in Industrie, Energiewirtschaft, Finanz- und Gesundheitswesen leiten, rund 2500 Risikomanager in mehrtägigen Weiterbildungslehrgängen qualifizieren und hunderte von Studierenden an der Technischen Hochschule in Deggendorf (Bayern) sowie an anderen Universitäten und Fachhochschulen unterrichten.

Dieses Buch ist ein Ergebnis langjähriger und zielgerichteter Arbeiten im Risikomanagement, wo sich nun Praxis und Theorie miteinander verbinden. Ich wünsche mir, dass viele Menschen an meinen Erkenntnissen und Erfahrungen teilhaben können.

Ein sehr herzliches Dankeschön gehört meiner lieben Doris. Sie hat mich – einmal mehr – mit ihren sprachlichen Fähigkeiten und mit dem seit vielen Jahren gewachsenen Verständnis für mein komplexes Fachgebiet tatkräftig unterstützt. Sie war auch bei dieser vierten, überarbeiteten Auflage des Buches unentbehrlich.

Zürich, im März 2016
Bruno Brühwiler