



— Frank Herdmann

# **Drei Schritte zum effektiven und effizienten Risikomanagement nach DIN ISO 31000**

Three Steps Starting Effective and Efficient  
Risk Management according to ISO 31000

**Drei Schritte zum effektiven und effizienten  
Risikomanagement nach DIN ISO 31000**

**Three Steps Starting Effective and Efficient  
Risk Management according to ISO 31000**

**(Leerseite)**



Frank Herdmann

**Drei Schritte zum effektiven  
und effizienten Risikomanagement  
nach DIN ISO 31000**

**Three Steps Starting Effective  
and Efficient Risk Management  
according to ISO 31000**

1. Auflage 2018  
1<sup>st</sup> edition 2018

Herausgeber/Edited by:  
DIN Deutsches Institut für Normung e.V.

Beuth Verlag GmbH · Berlin · Wien · Zürich

Herausgeber/Edited by: DIN Deutsches Institut für Normung e. V.

© 2018 Beuth Verlag GmbH

Berlin · Wien · Zürich

Am DIN-Platz

Burggrafenstraße 6

10787 Berlin

Telefon/Phone: +49 30 2601-0

Telefax/Fax: +49 30 2601-1260

Internet/Website: [www.beuth.de](http://www.beuth.de)

E-Mail/e-mail: [kundenservice@beuth.de](mailto:kundenservice@beuth.de)

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechts ist ohne schriftliche Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung in elektronische Systeme.

*All rights reserved. Without written permission from the publisher, no part of this book may be used for purposes not permitted by German copyright law, including duplication, translation, microform reproduction and electronic storage and processing.*

Die im Werk enthaltenen Inhalte wurden von Verfasser und Verlag sorgfältig erarbeitet und geprüft. Eine Gewährleistung für die Richtigkeit des Inhalts wird gleichwohl nicht übernommen. Der Verlag haftet nur für Schäden, die auf Vorsatz oder grobe Fahrlässigkeit seitens des Verlages zurückzuführen sind. Im Übrigen ist die Haftung ausgeschlossen.

*The contents of this work have been checked carefully by the authors and publisher, but no responsibility can be taken for their accuracy. The publisher accepts liability solely for damage caused by its own intent or gross negligence.*

- © für DIN-Normen DIN Deutsches Institut für Normung e. V., Berlin
- © Copyright for DIN Standards held by DIN Deutsches Institut für Normung e. V., Berlin

Titelbild/Cover picture/Coverdesign: © Fotolia, psdesign1

Satz/Typesetting: Sabine Wasser, Berlin

Druck/Printing: Drukarnia Leyko sp. z.o.o., Kraków

Gedruckt auf säurefreiem, alterungsbeständigem Papier nach DIN EN ISO 9706

*Printed on acid-free permanent paper as in DIN EN ISO 9706*

ISBN 978-3-410-28710-0

ISBN (E-Book) 978-3-410-28711-7

**Klippen umschiffen – Risiken managen**

**Avoid pitfalls – Manage risks**



# Content

	<b>Abbreviations</b> .....	4
	<b>Preface</b> .....	8
	<b>Introduction</b> .....	10
<b>1</b>	<b>Establishing the Framework</b> .....	28
<b>2</b>	<b>Establishing the Process</b> .....	40
<b>3</b>	<b>Implementing and Executing the RM Loop</b> .....	56
	<b>Annex: IIA fan</b> .....	68
	<b>Documents and Literature</b> .....	70
	<b>About the Author</b> .....	71
	<b>Acknowledgements</b> .....	72
	<b>Index</b> .....	74

## Abbreviations

- IEC** International Electrotechnical Commission, based in Geneva, Switzerland  
IEC is the world’s leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies.
- ISO** International Organization for Standardization, based in Geneva, Switzerland  
ISO is an independent, non-governmental international organization with a membership of 161 national standards bodies. Through their members, they bring together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.
- PDCA** Plan – Do – Check – Act; an iterative four step management concept for continuous improvement in business made popular by W.E. Deming
- SME** Small and Midsize Enterprises – the criteria differ from country to country; according to the European Commission the following criteria are applicable<sup>1</sup>:
- Micro: less than 10 employees and less than 2 million EUR turnover or balance sheet less than 2 million EUR
  - Small: less than 50 employees and less than 10 million EUR turnover or balance sheet less than 10 million EUR
  - Medium: less than 250 employees and less than 50 million EUR turnover or balance sheet less than 43 million EUR

---

1 Website of the European Commission:  
[http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index\\_en.htm](http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm)



## ABBREVIATIONS

---

- ISO/TC 262** ISO Technical Committee no. 262, responsible for standardization in the field of risk management
- ISO/TC 262 WG 2** Working group 2 of TC 262 titled *Core Risk Management Standards* and mandated with the revision of ISO 31000 (disbanded in 2018)
- ISO/TC 292** ISO Technical Committee no. 292, responsible for standardization in the field of security to enhance the safety and resilience of society

## Preface

Over the years the number of textbooks on the issues of risk management has been considerable. One might ask how necessary is a further book? In recent years, ISO 31000 has distinguished itself positively from other standards due to its practical relevance. This practical relevance is especially important for small and medium-sized enterprises which are still lacking in implementing a holistic risk management. With the concept of the event-driven process chain already in use in many companies, Frank Herdmann demonstrates how the implementation of a comprehensive risk management system can be designed. The standard will be soon adopted as a national German DIN standard and will be published in German. It therefore becomes necessary to further promote the implementation and integration of risk management into the corporate governance system.

The particular benefit of the present work lies, first, in the great topicality concerning the implementation of the new international standard for risk management, and additionally, in its bilingual approach of using the German and English languages. In particular for people who need to work in an international context or simply deal with risk management, this is a very good support for entry into this complex of topics.

I believe that this book can provide some ideas for setting up and developing a risk management system that will enable managers of small enterprises to deal professionally with the inevitable risks of doing business. In particular, the use of the event-driven process chain leads to a cost-efficient and effective implementation of the risk management process in companies.

I recommend this book for due attention from general managers, controllers, process owners and risk managers.

Berlin, May 2018

**Prof. Dr. Thomas Henschel, MBA (UK)**  
Hochschule für Technik und Wirtschaft Berlin