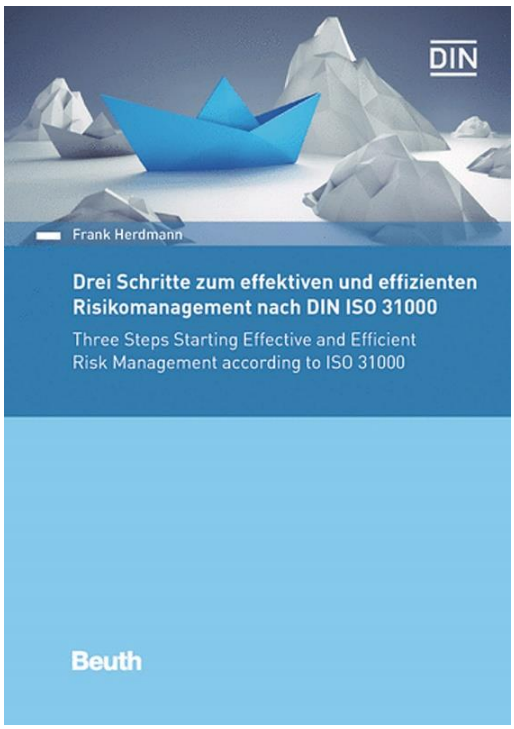
THREE STEPS STARTING EFFECTIVE AND EFFICIENT RISK MANAGEMENT ACCORDING TO ISO 31000

New Handbook explaining ISO 31000:2018

Over the years the number of textbooks on risk management has been considerable. ISO 31000 has distinguished itself from other standards due to its practical relevance. With its revision and publication of ISO 31000:2018 it has gained further practicability in particular for small and medium-sized enterprises which are still lacking in implementing a holistic risk management. In this handbook the author demonstrates how the implementation of a comprehensive risk management can be designed. With the new version of the standard having been adopted as a national German DIN standard published in German (D-A-CH translation jointly by the standardization bodies of Germany, Austria and Switzerland) this bilingual publication will be specifically useful for stakeholders working in an international environment. The purpose of risk management is the creation and protection of value and to prevent or at least reduce liabilities of management for organizational negligence! It is essential for good and responsible corporate governance and to avoid personal liability of leadership for organizational negligence.

Introduction

The introduction summarizes the history of risk management and briefly introduces ISO 31000:2009 and its overwhelming success. The standard has been adopted by more than 60 national standardization organizations as national standard.



Rationale of the Handbook

The objective of the handbook is to give a quick first access to risk management in particular for smaller or midsize enterprises. It is not aiming to give perfect guidance down to the last detail for large organizations with complex structure and business. Detailed advice will not be needed for first steps, but first steps will be needed if the organization doesn't have any risk management or if it has an outdated risk management that is restricted to periodical data collection.

For large and complex organizations this will be just a fast-initial start allowing for a more mature risk management to follow with time – for small enterprises it might be the needed customized approach.

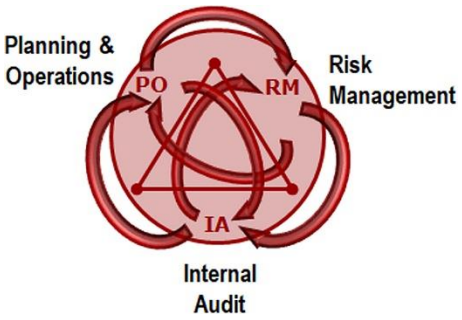
The three Steps

- **Establishing the framework:** The Framework should be customized for the organization. Special attention must be given to leadership and commitment and human and cultural factors (e.g. the ETTO principle) should be considered. Integrating risk management into an organization is a dynamic and iterative process customized to the organization's needs and culture.

- **Establishing the Process:** The risk management process should be an integral part of management and integrated into the structure, operations and processes of the organization – in short into all its activities. The core of the risk management process is basically a four-item loop starting with risk identification followed by risk analysis, risk evaluation and risk treatment. The »Event-driven Process Chain« (EPC), a popular tool of business economists in Central Europe, is used to illustrate the loop. It is emphasized that the risk management process even if mostly shown in sequential figures has in fact an iterative nature. For the reporting system it should be noted that less might be more and a highly differentiated reporting might create confusion and a false notion of security.
- **Implementing and Executing the Risk Management Loop:** To activate synergies and to reduce efforts and expenses it is suggested to consider the risk management loop in the context of designing and implementing the organization's core business processes which might be collected in an organizational manual. The loop should be plugged into the processes whenever any information or estimation is starting a process and it should be repeated whenever any additional information and/or new estimation affects the business process. The task owner who will be the risk owner for this part of the business process is advised to consider whether an uncertainty might affect the process and the achievement of objectives.

Internal Audit

One important item will be aligning risk management with internal audit as part of integrating risk management in all activities and processes. This is a two-way approach also affecting planning and operations. Internal Audit will monitor the execution of the risk management loop as it will monitor all business activities of the organization. On the other hand, the results of risk management will be the basis for the periodic planning of Internal Audit.



Continual Improvement

Applying the PDCA Cycle advocated by Deming will improve and refine the risk management loop over time and achieve higher levels of maturity of the organization's risk management. Risk management like any other skill will not fall out of the sky but takes training and experience and is open to continual improvement as envisioned by the PDCA-Cycle.

The handbook (bilingual English-German) is made available by Beuth publishing

For more information contact the author: auxilium@herdmann.de

Dr. Frank Herdmann | Gluckweg 10 | 12247 Berlin | Germany | phone: +49 30 771 90 321