

Abstract of an article in **ZRFC** 3/2018 (June 2018) pg. 111 ff ◀▶ Authors are Dr. Frank Herdmann, Vice Chair of DIN NA 175-00-04 AA, the German mirror committee to ISO/TC 262, who had been the head of the German delegation to TC 262 during the revision of the standard and Prof. Dr. Thomas Henschel, Professor for business economics, in particular accounting and compliance at HTW (Hochschule für Technik und Wirtschaft in Berlin)

FEASIBLE RISK MANAGEMENT FOR SMEs IN GERMANY ISO 31000 ADOPTED BY DIN AS A NATIONAL STANDARD

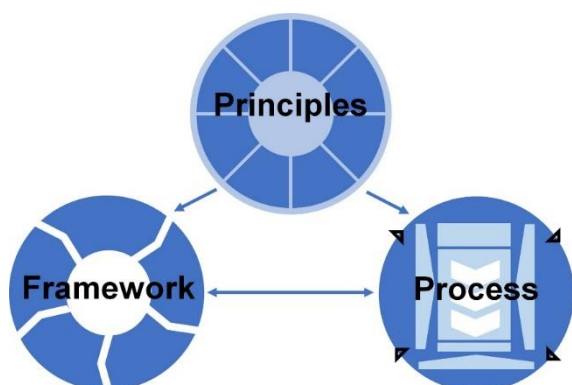
Introduction and conclusion

The article recently published in ZRFG 3/18 (Zeitschrift Risk, Fraud & Compliance) explains the development of risk management in Germany since the beginning of the 20th century including its current legal background. This is followed by a description of the development from ISO 31000:2009 to ISO 31000:2018 and DIN ISO 31000:2018. While ISO 31000:2009 developed globally to become the leading risk management standard being adopted as a national standard in more than 60 countries, it was not adopted in Germany by DIN.

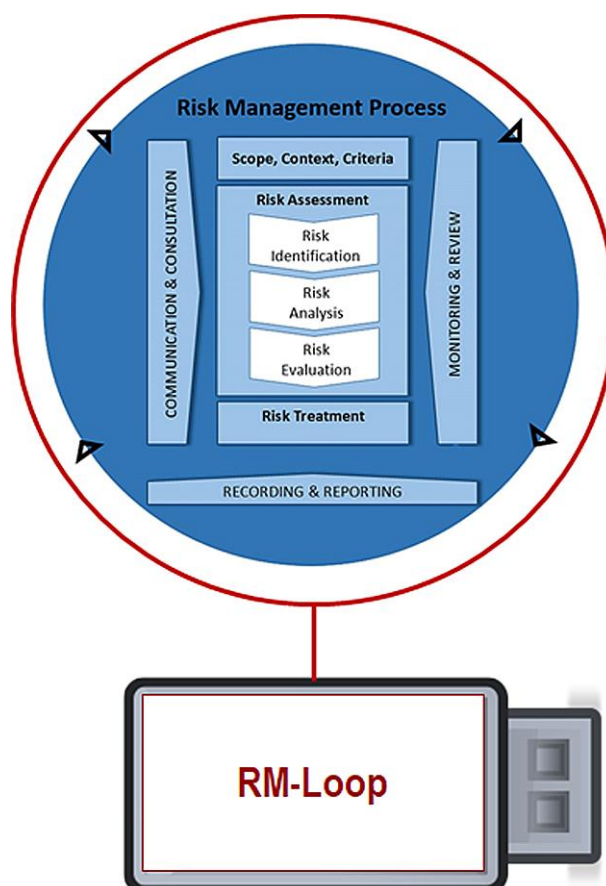
While empirical research showed improvements in the risk management of owner managed SMEs in Germany, there was considerable potential for improvement to be found. It is asserted that the revision and streamlining of ISO 31000 resulted in a cost efficient and effective tool for SMEs for the implementation of a holistic risk management in the organization. As the revised standard has been adopted by DIN as a national standard (publication is expected for October) SMEs in Germany now have guidance for the implementation of risk management. The concept of integration into the organization's management system supports the use of the standard for SMEs. Risk management is no longer a time consuming additional task but a chance to enhance the processes of the enterprise.

From ISO 31000:2009 to DIN ISO 31000:2018 – Principles and Process

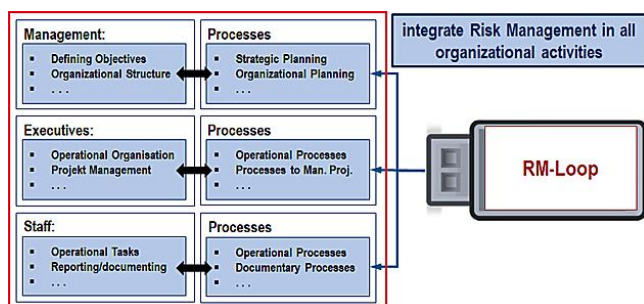
The article explains the three-pillar-structure of the standard and its sections on principles and process.



It emphasizes the creation and protection of value as the central concept leading the clause on principles with principle a (integrated) and principle c (customized) being the two most important principles. Principle a) documents the vital step from a reactive just documenting risk reporting to an active risk treatment. The process is compared to a loop that can be used like a plug-in dongle that enhances the activities of the organization that can be compared to a computer with CPUs for its various activities/processes.



The integration of risk management into all organizational activities



By mapping the risk management process in the form of an event driven process chain it can be easily integrated into the organizational processes identically mapped. The integration of risk management becomes the expansion of the relevant process chain by the (iterative) steps of the risk management process. Each process owner becomes the risk owner responsible for managing the risks within the processes in his or her responsibility and accountability. Risk management is the responsibility of every member or the organization starting with top management.



Consequences of adopting ISO 31000:2018 as a national standard in Germany

With the adoption of ISO 31000:2018 as a national standard by DIN German companies become end-users of the standard without having to construe its applicability by best practice rules. As before being a generic guidance standard it is not for certification. It does not use the term »risk manager«. And as there is no such separate role companies should not employ risk managers. The risk owner will have to assess and treat risks. In big, complex organizations a risk officer might be responsible for training/coaching risk owners and support the aggregation of risk positions within the risk reporting. The overall responsibility for risk management will remain with top management.

Integration and Management Systems

As all important aspects of managing a company can be part of a management system integrating the organization's management systems into one holistic system prevents the development of silos of responsibilities. ISO has developed with its High-Level Structure (HLS) in annex SL appendix 2 a tool for easily integrating management systems. The HLS includes the requirement to use an approach based on risk management (the so-called risk-based approach). In this context the risk management loop can be reused repeatedly as a plug-in dongle – provided that principle c) customizing is observed. Applying ISO 31000 will enable the end-user to integrate risk management into the integrated holistic management system of the organization and all its organizational activities in pursuing its objectives.