ISO/ANSI/ASSE Technical Report

ISO/ANSI/ASSE TR-31004-2014

National Adoption of:
ISO/TR 31004:2013

Risk Management—Guidance for the Implementation of ISO 31000

ISO/ANSI/ASSE TR-31004-2014

American Society of Safety Engineers
1800 East Oakton Street
Des Plaines, IL 60018
www.asse.org

The information and materials contained in this publication have been developed from sources believed to be reliable. However, the American Society of Safety Engineers (ASSE) as secretariat of the ANSI accredited Z690 Committee or individual committee members accept no legal responsibility for the correctness or completeness of this material or its application to specific factual situations. By publication of this standard, ASSE or the Z690 Committee does not ensure that adherence to these recommendations will protect the safety or health of any persons, or preserve property.

ISO/ANSI/ASSE TR-31004 – 2014

National Adoption of:
ISO/TR 31004:2013

ISO/ANSI/ASSE Technical Report

Risk Management – Guidance for the Implementation of ISO 31000

Prepared by the American Society of Safety Engineers

Secretariat and Standards Developing Organization:

American Society of Safety Engineers
1800 East Oakton Street
Des Plaines, Illinois 60018-2187
(847) 699-2929 • www.asse.org

Published May, 2014

Printed in the United States of America

FOREWORD

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the Foreword – Supplementary information page of the www.iso.org website.

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Developer, American Society of Safety Engineers (ASSE), 1800 E. Oakton Street, Des Plaines, Illinois 60018. This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to the American Society of Safety Engineers, Attention: Secretariat, 1800 E. Oakton Street, Des Plaines, Illinois 60018.

The committee responsible for this document is Technical Committee ISO/TC 262, Risk management.

At the time this technical report was published, the United States Technical Advisory Group/Committee had the following members:

Dorothy Gjerdrum, ARM-P, Chair
Carol Fox, Vice Chair
Timothy R. Fisher, CSP, CHMM, ARM, CPEA, Administrator
Jennie Dalesandro, Administrative Technical Support

Organization Represented	Name of Representative
AH&T Insurance	Mike DeRosier
AIHA	Paul A. Esposito, CIH, CSP, CPEA
	David Hicks
American Broadcasting Companies, Inc.	Michael Miller
American Society of Safety Engineers	James Newberry
	Francis Sehn, CSP, ARM

ARCADIS	Tom Burgess
	Danyle Hepler, CSP
Arthur J. Gallagher & Co.	Dorothy Gjerdrum, ARM-P
	James D. Smith, CSP
Bayer MaterialScience	Terry L. Ketchum
Brazosport College	Craig E. Litton, Dr.P.H.
CNA Insurance	Bill Boyd
	Joel Schneider
Deloitte & Touche LLP	Jeffrey DeRose
	Kim A. Detiveaux
Eide Bailly, LLP	Mary Peter
	Chelsie Cheney, CPA
Erachem Comilog Inc.	Victor S. Klein
	Hector E. Rojas
ERM31000 Consulting	Allen Gluck
ESIS Inc.	Robert Wayne Clifton
	Steve DiPilla
Kleinfelder	Scott Dwyer
	Steve Ackerlund
MC Dean, Inc.	John Bennett
	James Kohlmeyer
Packaging Machinery Manufacturers Institute	Fred Hayes
	Bruce W. Main, P.E., CSP
Pfizer Inc.	Steven Meszaros
	Steve Moore
Project Management Institute	Karl Best
	John Zlockie
Public Risk Management Association	Matt Hansen
	Marshall Davies
Risk Management & Insurance Society	Carol Fox
	Chris O'Donnell
SAP	Norman Marks
Schanfield Risk Management Advisors LLC	Arnold Schanfield, CPA, CIA, CFE
URS	William Piispanen, CIH, CSP, CEA
U.S. Department of Commerce	Karen Hardy, Ed.D.
U.S. Department of Energy (BPA)	Ryan Egerdahl
	Erik Westman
U.S. Department of Homeland Security	Patricia Underwood
U.S. Department of Veterans Affairs	Catherine Chatfield, PMP, CBCP, ARM-E
University of California	Carrie Frandsen, ARM
	Erike Young, MPPA, CSP, ARM

Contents

Introduction

0.1 General

Organizations use various methods to manage the effect of uncertainty on their objectives, i.e. to manage risk, by detecting and understanding risk, and modifying it where necessary.

This Technical Report is intended to assist organizations to enhance the effectiveness of their risk management efforts by aligning them with ISO 31000:2009. ISO 31000 provides a generic risk management approach that can be applied to all organizations to help achieve their objectives.

This Technical Report is intended to be used by those within organizations who make decisions that impact on achieving its objectives, including those responsible for governance and those who provide organizations with risk management advice and support services. This Technical Report is also intended to be used by anyone interested in risk and its management, including teachers, students, legislators and regulators.

This Technical Report is intended to be read in conjunction with ISO 31000 and is applicable to all types and sizes of organization. The core concepts and definitions that are central to understanding ISO 31000 are explained in Annex A.

Clause 3 provides a generic methodology to help organizations transition existing risk management arrangements to align with ISO 31000, in a planned and structured way. It also provides for dynamic adjustment as changes occur in the internal and external environment of the organization.

Additional annexes provide advice, examples and explanation regarding the implementation of selected aspects of ISO 31000, in order to assist readers according to their individual expertise and needs.

Examples provided in this Technical Report might or might not be directly applicable to particular situations or organizations, and are for illustrative purposes only.

0.2 Underlying concepts and principles

Certain words and concepts are fundamental to understanding both ISO 31000 and this Technical Report, and they are explained in ISO 31000:2009, Clause 2, and in Annex A.

ISO 31000 lists eleven principles for effective risk management. The role of the principles is to inform and guide all aspects of the organization’s approach to risk management. Principles describe the characteristics of effective risk management. Rather than simply implementing the principles, it is important that the organization reflects them in all aspects of management. They serve as indicators of risk management performance and reinforce the value to the organization of managing risk effectively. They also influence all elements of the transition process described in this Technical Report, and the technical issues that are the subject of its annexes. Further advice is given in Annex B.

In this Technical Report, the expressions “top management” and “oversight body” are both used: “top management” refers to the person or group of people that directs and controls an organization at the highest level, whereas “oversight body” refers to the person or group of people that governs an organization, sets directions, and holds top management to account.

NOTE In many organizations, the oversight body could be called a board of directors, a board of trustees, a supervisory board, etc.

ISO/ANSI/ASSE TECHNICAL REPORT TR-31004-2014
RISK MANAGEMENT –
GUIDANCE FOR THE IMPLEMENTATION OF ISO 31000

1 Scope

This Technical Report provides guidance for organizations on managing risk effectively by implementing ISO 31000:2009. It provides:

— a structured approach for organizations to transition their risk management arrangements in order to be consistent with ISO 31000, in a manner tailored to the characteristics of the organization;

— an explanation of the underlying concepts of ISO 31000;

— guidance on aspects of the principles and risk management framework that are described in ISO 31000.

This Technical Report can be used by any public, private or community enterprise, association, group or individual.

NOTE For convenience, all the different users of this Technical Report are referred to by the general term “organization”.

This Technical Report is not specific to any industry or sector, or to any particular type of risk, and can be applied to all activities and to all parts of organizations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000:2009, *Risk management — Principles and guidelines*

3 Implementing ISO 31000

3.1 General

This clause provides guidance to organizations seeking to align their risk management approach and practices with ISO 31000 and to maintain those practices in alignment on an ongoing basis.

It provides a general methodology that is suitable for application, in a planned manner, by any organization irrespective of the nature of its current risk management arrangements. This methodology involves the following: