ANSI/ASSP/ISO 31000-2018

Risk Management – Guidelines

AMERICAN SOCIETY OF
SAFETY PROFESSIONALS

ANSI®
ANSI/ASSP/ISO 31000 – 2018

American National Standard

Risk Management – Guidelines

Secretariat

American Society of Safety Professionals
520 N. Northwest Highway
Park Ridge, Illinois 60068

Approved July 20, 2018

American National Standards Institute

American National Standard

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus and other criteria for approval have been met by the standards developer. Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution. The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he/she has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards. The American National Standards Institute does not develop standards and will in no circumstance give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretation should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

Caution Notice: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Published August 2018 by

American Society of Safety Professionals
520 N. Northwest Hwy
Park Ridge, IL 60068
(847) 699-2929 • www.assp.org

Printed in the United States of America

Foreword

(This Foreword is not a part of American National Standard ANSI/ASSP/ISO 31000-2018.)

This standard provides general guidelines for risk management. The standard was developed by an American National Standards Committee (United States Technical Advisory Group to ANSI for ISO/TC 262), in concert with the standards organizations and liaisons of TC 262 acting within the ISO Directives. The committee, which is national in scope, functions under the Essential Requirements Document of the American National Standards Institute with the American Society of Safety Professionals (ASSP) as Secretariat.

This standard is an identical adoption of the ISO 31000:2018, an international standard also titled "Risk management – Guidelines." The document was approved as an international standard in February 2018.

This standard replaces American National Standard ANSI/ASSP Z690.2-2011. Those organizations that currently are using the ANSI/ASSP Z690.2-2011 standard as guidance for risk management will benefit from considering the shift in perspective for full integration that is key to the revised 2018 version of the standard.

The standard now includes purpose statements of risk management and each of the components: principles, framework and process. Recognizing that organizations may already have a set of principles, a framework and process for managing risk, the content has been streamlined to encourage users to customize and improve how they manage risk through the updated standard's guidance.

The standard establishes the creation and protection of value as the core purpose of risk management and includes eight principles that are designed to help organizations improve performance, encourage innovation and support the achievement of objectives.

The standard places an increased emphasis on integrating risk management into all organizational activities, processes and decision-making within the framework. It also emphasizes that top management is accountable for managing risk while oversight bodies are accountable for overseeing risk management.

The standard explicitly states that the process is iterative in practice by decision-makers and affected stakeholders. This statement stresses the importance of managing risk when decisions are being made, rather than as an afterthought or as an additional step after decisions already are made.

At the time this standard was approved, the Technical Advisory Group/Committee had the following members:

Carol Fox, Chair
Erike Young, CSP, ARM-E, Vice Chair
Lauren Bauerschmidt, MS Engr, CSP, STS, Secretary
Ovidiu Munteanu, Assistant Secretary
Jennie Dalesandro, Administrative Technical Support

Organization Represented	Name of Representative
American Industrial Hygiene Association	Paul Esposito, CIH, CSP
American Society of Safety Professionals	James Newberry
	Francis Sehn, CSP, ARM
Arcadis	Sandra Johnston
	Aaron Neal
ARM Study Group	Erike Young, CSP, ARM-E
Arthur J. Gallagher & Co.	Dorothy Gjerdrum, ARM-P
	Joey Sylvester

ASSP Risk Assessment Institute	Kenneth Daigle
	Paul Zoubek
Brazosport College	Samuel Chamberlain, M.S.
	Craig Litton, Dr.P.H.
Cincinnati Insurance Company	Kevin Oleckniche, M.S., CPCU, ARM, CSP
	Jeff Spangler
CNA	Jonelle Dubois
	Lesli Johnson
ERM31000 Training & Consulting	Allen Gluck
ESIS Inc.	Steven Di Pilla, ARM, CSP
	Ellen McBride
Forensic Investigations and Technologies	Charles Coones
Google Inc.	Jim Campbell
Hays Companies	Bruce Lyon
M. Siegel Associates LLC	Marc Siegel
M.C. Dean, Inc.	John Bennett, CHCM
	Aaron Schoemaker, CSP
Oracle	Lianne Appelt, Sc.D.
	Amita Radhakrishnan
Pfizer Inc.	Steven Meszaros
	Steve Moore
Project Management Institute, Inc.	Marvin Nelson, MBA, CAE, SCPM
	John Zlockie
Public Risk Management Association	Scott Moss
	Marshall Davies
RIMS	Carol Fox
	Randy Jouben, CPCU, ARM, CBCP, MBCI
State Office of Risk Management	James Cox
	Stephen Vollbrecht, J.D.
University of California	Carrie Frandsen, ARM-E
	Tim Willette
University of Central Missouri	Georgi Popov, Ph.D., ARM, SMS, QEP
Young Life	Gary Nesbit, CSP, ARM, AIC, ALCM, SPHR, CPCU

Contents

Page

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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www. iso. org/iso/foreword. html.

This document was prepared by Technical Committee ISO/TC 262, *Risk management*.

This second edition cancels and replaces the first edition (ISO 31000:2009) which has been technically revised.

The main changes compared to the previous edition are as follows:

— review of the principles of risk management, which are the key criteria for its success;

— highlighting of the leadership by top management and the integration of risk management, starting with the governance of the organization;

— greater emphasis on the iterative nature of risk management, noting that new experiences, knowledge and analysis can lead to a revision of process elements, actions and controls at each stage of the process;

— streamlining of the content with greater focus on sustaining an open systems model to fit multiple needs and contexts.

Introduction

This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.

Organizations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives.

Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.

Managing risk is part of all activities associated with an organization and includes interaction with stakeholders.

Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

Managing risk is based on the principles, framework and process outlined in this document, as illustrated in Figure 1. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective and consistent.

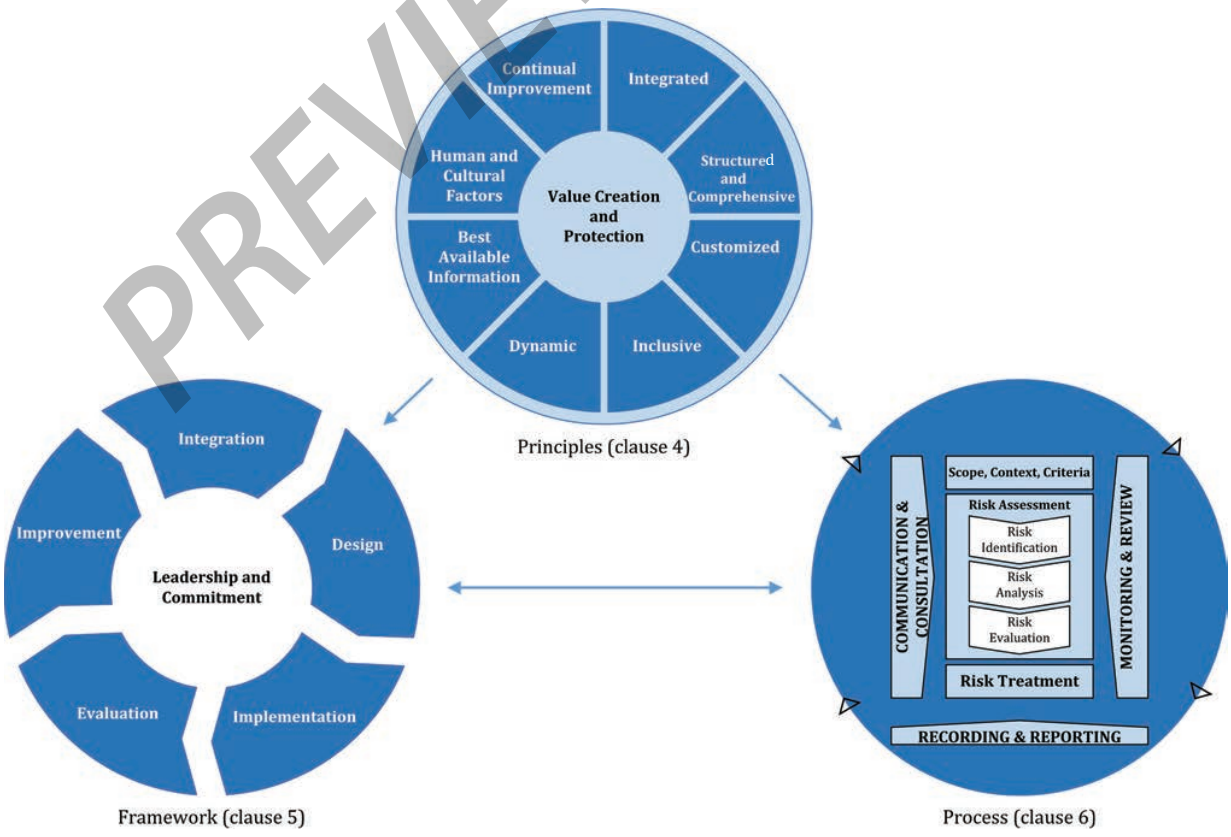

Figure 1 — Principles, framework and process

Page Intentionally Left Blank

Risk management — Guidelines

1 Scope

This document provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

This document provides a common approach to managing any type of risk and is not industry or sector specific.

This document can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org

3.1
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of *risk sources* (3.4), potential *events* (3.5), their *consequences* (3.6) and their *likelihood* (3.7).

3.2
risk management
coordinated activities to direct and control an organization with regard to *risk* (3.1)

3.3
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: The term “interested party” can be used as an alternative to “stakeholder”.

3.4
risk source
element which alone or in combination has the potential to give rise to *risk* (3.1)