

ANSI/ASSP Z690.2-2011

Risk Management - Principles and Guidelines (National Adoption of ISO 31000:2009)

The American Society of Safety Engineers (ASSE) is now the American Society of Safety Professionals (ASSP). ASSP continues to be the Secretariat for the committee producing this standard and continues to hold the copyright to this standard. There is no change to the content and requirements in the standard. The only change is on the cover indicating the organizational name change of the standards developing organization from ASSE to ASSP.



**AMERICAN SOCIETY OF
SAFETY PROFESSIONALS**

Copyright American Society of Safety Professionals
Provided by IHS Markit under license with ASSE/SAFE
No reproduction or networking permitted without license from IHS
Full document details: ASSP Z690.2 2011

Licensee=/, User=,
Not for Resale,



— — — — —

ANSI®
ANSI/ASSE/ISO 31000 (Z690.2-2011)

National Adoption of:
ISO 31000:2009

American National Standard

Risk Management Principles and Guidelines

Secretariat

American Society of Safety Engineers
1800 East Oakton Street
Des Plaines, Illinois 60018-2187

Approved: January 11, 2011

American National Standards Institute, Inc.

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 requires 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 February 2011 by:

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

Copyright © 2011 by the American Society of Safety Engineers
All Rights Reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Printed in the United States of America

Foreword (This Foreword is not a part of American National Standard Z690.2-2011.)

This standard was developed by an American National Standards Committee, national in scope, functioning under the Essential Requirements Document of the American National Standards Institute with the American Society of Safety Engineers (ASSE) as Secretariat. This standard provides risk management principles and guidelines

It is intended that the procedures and performance requirements detailed herein will be adopted by every employer whose operations fall within the scope and purpose of the standard.

Neither the standards committee, nor the secretariat, feel that this standard is perfect or in its ultimate form. It is recognized that new developments are to be expected, and that revisions of the standard will be necessary as the art progresses and further experience is gained. It is felt, however, that uniform requirements are very much needed and that the standard in its present form provides for the minimum performance requirements necessary in developing and implementing risk management programs.

This standard is adopted from ISO 31000:2009, an international standard also titled "Risk Management Principles and Guidelines". This document was approved as an international standard on November 15, 2009. In addition to ISO 31000 there are also two other documents addressing risk management and risk assessment being adopted as American National Standards:

ISO Guide 73:2009, *Risk Management - Vocabulary*

IEC/ISO 31010:2009, *Risk Management – Risk Assessment Techniques*

During May 2010 the United States TAG (Technical Advisory Group) to ANSI for risk management reached consensus that these three documents should be adopted as American National Standards. Due to the ongoing significant interest being focused on risk management at the international level, additional consensus was reached that there should also be a committee looking at risk management standards for the United States. Such a committee would function under accreditation of ASSE as a standards developing organization (SDO).

ASSE applied for additional accreditation as a Standards Developing Organization, which was approved by ANSI during August of 2010. ASSE notified the public during August 2010 of its intention to adopt all three documents as American National Standards. This original announcement was made without the submission of any negative comments. Public review of the subject documents was then conducted during November 2010. There were no negative comments submitted to ASSE as the secretariat. All committee votes for adoption were positive without any submitted negative comments.

At the time this standard was approved, the 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

George Forrester

American Society of Safety Engineers

Paul A. Esposito, CIH, CSP, CPEA

Arthur J. Gallagher & Co.

Benjamin Heckman, MPH, CIH

Bayer MaterialScience

Leslie M. Batterson, CSP, CPEA

Brazosport College

James Newberry

Eide Bailly, LLP

Dorothy Gjerdrum, ARM-P

James D. Smith, CSP

Terry L. Ketchum

Craig E. Litton, Dr.P.H.

Mary Peter

Karen Peterka

ESIS Inc.

Robert Wayne Clifton

Steve DiPilla

McCulley, Eastham & Associates

L. Todd Eastham

Packaging Machinery Manufacturers Institute

Fred Hayes

Bruce W. Main, P.E., CSP

Pilz Automation Safety, L.P.

Gilbert Dominguez

Craig Torrance

Project Management Institute

Karl Best

John Zlockie

Public Risk Management Association

Matt Hansen

Risk Management & Insurance Society

Carol Fox

Chris O'Donnell

Safety Management Consultants, Inc.

J. Terrence Grisim, CSP, CDS,

CPSM, ARM

URS

Mary Ellen Grisim, ARM

U.S. TAG to ISO/TC 176

William Piispanen, CIH, CSP, CEA

Woods Hole Oceanographic Institution

John Walz

Ron Reif

Wyeth

Georgi Crowley

Steven Meszaros

Alan Moran

Significant Contributor:

Wayne L. Salen, ARM, CHCM, CPSM

Introduction

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is "risk".

All activities of an organization involve risk. Organizations manage risk by identifying it, analyzing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this standard establishes a number of principles that need to be satisfied to make risk management effective. This standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this standard is the inclusion of "establishing the context" as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this standard are shown in Figure 1.

When implemented and maintained in accordance with this standard, the management of risk enables an organization to, for example:

- increase the likelihood of achieving objectives;
- encourage proactive management;
- be aware of the need to identify and treat risk throughout the organization;
- improve the identification of opportunities and threats;
- comply with relevant legal and regulatory requirements and international norms;
- improve mandatory and voluntary reporting;

- improve governance;
- improve stakeholder confidence and trust;
- establish a reliable basis for decision making and planning;
- improve controls;
- effectively allocate and use resources for risk treatment;
- improve operational effectiveness and efficiency;
- enhance health and safety performance, as well as environmental protection;
- improve loss prevention and incident management;
- minimize losses;
- improve organizational learning; and
- improve organizational resilience.

This standard is intended to meet the needs of a wide range of stakeholders, including:

- a) those responsible for developing risk management policy within their organization;
- b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;
- c) those who need to evaluate an organization's effectiveness in managing risk; and
- d) developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this standard.

In this standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, while “managing risk” refers to applying that architecture to particular risks.

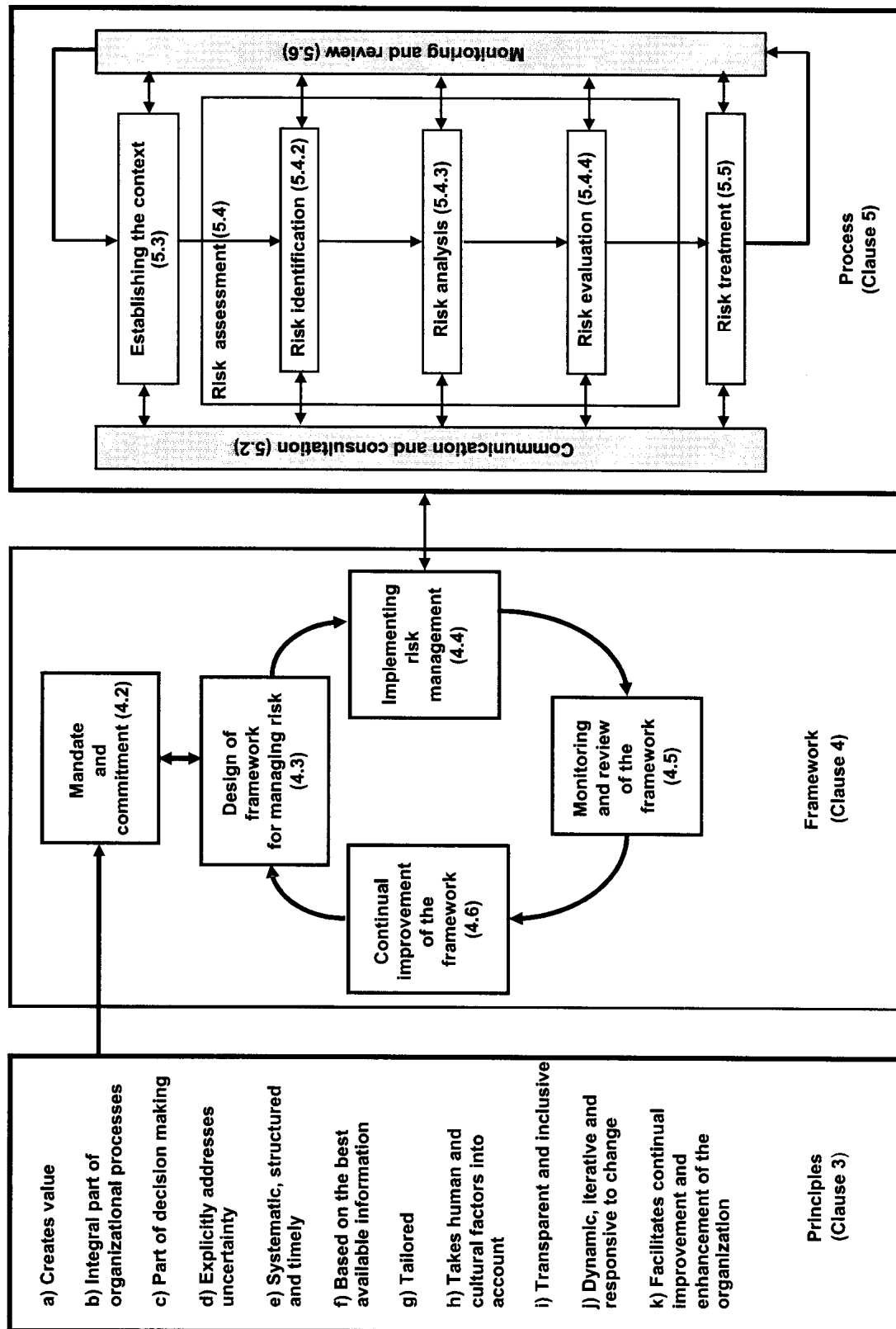


Figure 1 – Relationships Between the Risk Management Principles, Framework and Process

Contents	SECTION	PAGE
1. Scope		10
2. Terms and Definitions		10
3. Principles		14
4. Framework		15
4.1 General		15
4.2 Mandate and Commitment		16
4.3 Design of Framework for Managing Risk		17
4.4 Implementing Risk Management		19
4.5 Monitoring and Review of the Framework		20
4.6 Continual Improvement of the Framework		20
5. Process		20
5.1 General		20
5.2 Communication and Consultation		21
5.3 Establishing the Context		22
5.4 Risk Assessment		24
5.5 Risk Treatment		26
5.6 Monitoring and Review		27
5.7 Recording the Risk Management Process		28
Annex A – Attributes of Enhanced Risk Management		29
Bibliography		31

AMERICAN NATIONAL STANDARD Z690.2 RISK MANAGEMENT PRINCIPLES AND GUIDELINES

1. SCOPE

This standard provides principles and generic guidelines on risk management.

This standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this standard is not specific to any industry or sector.

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

This standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This standard is not intended for the purpose of certification.

2. TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions apply. These terms and definitions are taken from ANSI/ASSE Z690.1, *Vocabulary for Risk Management*. (ISO Guide 73:2009)

2.1 Communication and Consultation. Continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk.

NOTE 1: The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk.

NOTE 2: Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

- a process which impacts on a decision through influence rather than power; and
- an input to decision making, not joint decision making.

2.2 Consequence. Outcome of an event affecting objectives.

NOTE 1: An event can lead to a range of consequences.

NOTE 2: A consequence can be certain or uncertain and can have positive or negative effects on objectives.