SVENSK STANDARD
SS-ISO 31000:2018

Fastställd/Approved: 2018-04-05
Publicerad/Published: 2018-04-11
Utgåva/Edition: 2
Språk/Language: svenska/Swedish, engelska/English
ICS: 03.100.01

Riskhantering – Vägledning (ISO 31000:2018, IDT)

Risk management – Guidelines (ISO 31000:2018, IDT)

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Den internationella standarden ISO 31000:2018 gäller som svensk standard. Detta dokument innehåller den svenska språkversionen av ISO 31000:2018 följd av den officiella engelska språkversionen.

Denna standard ersätter SS-ISO 31000:2009 utgåva 1.

The International Standard ISO ISO 31000:2018 has the status of a Swedish Standard. This document contains the Swedish language version of ISO 31000:2018 followed by the official English version.

This standard supersedes the Swedish Standard SS-ISO 31000:2009, edition 1.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för Samhällssäkerhet, SIS/TK 494.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Innehåll

Sida

Förord

ISO (Internationella Standardiseringsorganisationen) är en världsomspännande sammanslutning av nationella standardiseringsorgan (ISO-medlemmar). Utarbetandet av internationella standarder sker normalt i ISOs tekniska kommittéer. Varje medlemsland som är intresserat av arbetet i en teknisk kommitté har rätt att bli medlem i den. Internationella organisationer, statliga såväl som icke-statliga, som samarbetar med ISO deltar också i arbetet. ISO har nära samarbete med International Electrotechnical Commission (IEC) i alla frågor rörande elektroteknisk standardisering.

De förfaranden som har tillämpats vid framtagningen av det här dokumentet samt de som ska tillämpas vid uppdatering beskrivs i ISO/IEC-direktiven, Del 1. De olika godkännandekriterier som gäller för olika typer av ISO-dokument bör efterlevas särskilt. Det här dokumentet har utformats i enlighet med de redaktionella reglerna i ISO/IEC-direktiven, Del 2 (se www.iso.org/directives).

Observera att vissa delar av detta dokument kan omfattas av patenträttigheter. ISO ansvarar inte för identifiering av sådana patenträttigheter. Information om eventuella patenträttigheter som har identifierats under arbetet med dokumentet finns i avsnittet Orientering och/eller ISO:s förteckning över mottagna patent (se www.iso.org/patents).

Alla varumärken som används i det här dokumentet ges i informationssyfte för att underlätta för användaren, men kan inte garanteras.

En förklaring av frivilligheten kring standarder, ISO-specifika termer och uttryck med relevans för bedömningen av överensstämmelse, samt information om ISO:s efterlevnad av Världshandelsorganisationen WTO:s principer enligt avtalet om tekniska handelshinder (Technical barriers to trade, TBT) finns här: www.iso.org/iso/foreword.html.

Detta dokument har utarbetats av den tekniska kommittén ISO/TC 262, Risk management.

Denna andra utgåva upphäver och ersätter den första utgåvan (ISO 31000:2009) som har blivit tekniskt reviderad.

De huvudsakliga förändringarna från föregående utgåva är:

– Granskning av principerna för riskhantering, vilka är de viktigaste kriterierna för framgång.

– Fokus på högsta ledningens ledarskap, och integrering av riskhantering med utgångspunkt i organisationens verksamhetsstyrning.

– Större fokus på riskhanteringens iterativa egenskaper, med hänsyn till att nya erfarenheter, kunskap och analys kan leda till en ändring av processens delmoment, aktiviteter och åtgärder inom varje steg av processen.

– Förenkla innehållet med större fokus på att bibehålla en öppen systemmodell som kan tillgodose flera behov och förutsättningar.

Orientering

Detta dokument är avsett att användas av personer som skapar och skyddar en organisations värden genom att hantera risker, fatta beslut, sätta upp mål och uppnå dem, samt förbättra resultaten.

Organisationer av alla typer och storlekar ställs inför både externa och interna faktorer och influenser som bidrar till osäkerhet om huruvida de kommer att uppnå sina mål.

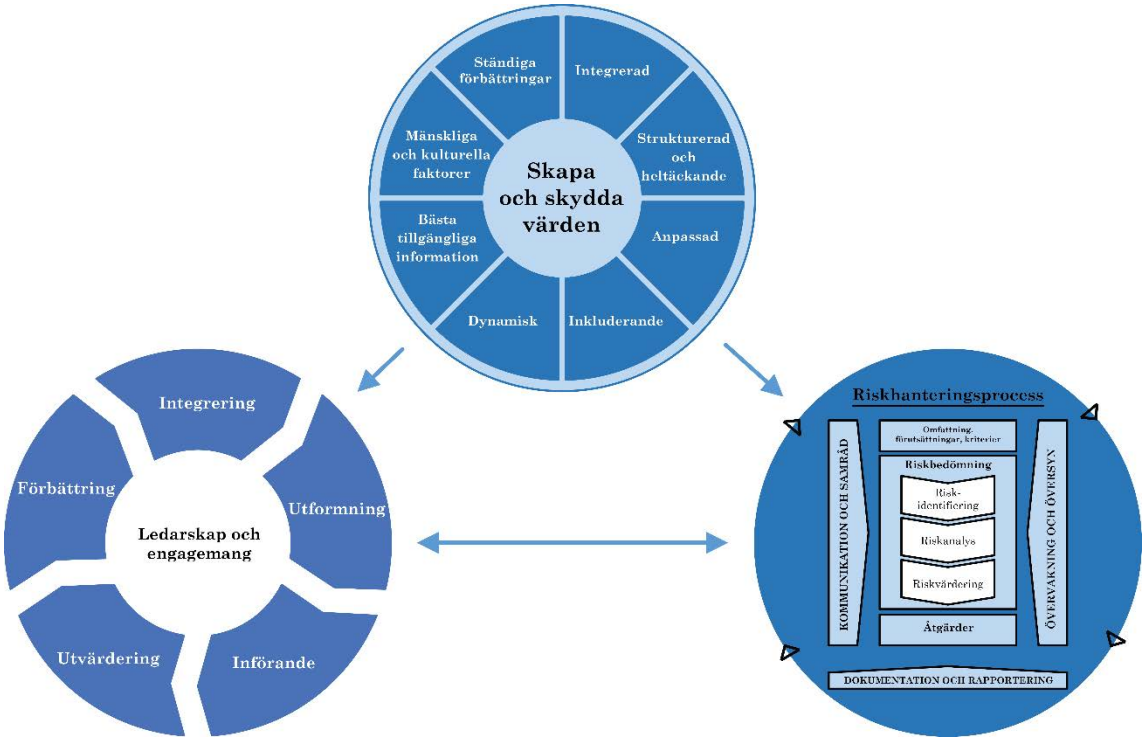
Riskhantering är en iterativ process som hjälper organisationer att fastställa strategier, uppnå mål och fatta välgrundade beslut.

Riskhantering är en del av styrningen och ledarskapet och är avgörande för hur organisationen styrs på alla nivåer. Den bidrar till att förbättra ledningssystemen.

Riskhantering ingår i en organisations samtliga aktiviteter och omfattar även kontakten med intressenter.

Riskhantering tar hänsyn till organisationens externa och interna förutsättningar, inklusive mänskliga beteenden och kulturella faktorer.

Riskhantering bygger på de principer, ramverk och processer som beskrivs i detta dokument, enligt Figur 1. Dessa komponenter kan, i sin helhet eller delvis, redan finnas inom organisationen. De kan dock behöva anpassas eller förbättras så att risker hanteras på ett effektivt, verkningsfullt och konsekvent sätt.



Figur 1 – Principer, ramverk och process

1 Omfattning

Detta dokument innehåller riktlinjer för att hantera de risker som en organisation ställs inför. Tillämpningen av dessa riktlinjer kan anpassas efter organisationen och dess förutsättningar.

Detta dokument tillhandahåller en gemensam strategi för att hantera alla typer av risker och är inte specifikt utformat för någon bransch eller sektor.

Detta dokument kan tillämpas under en organisations hela livslängd och på alla typer av aktiviteter, inklusive beslutsfattande på alla nivåer.

2 Normativa hänvisningar

Detta dokument innehåller inga normativa hänvisningar.

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.

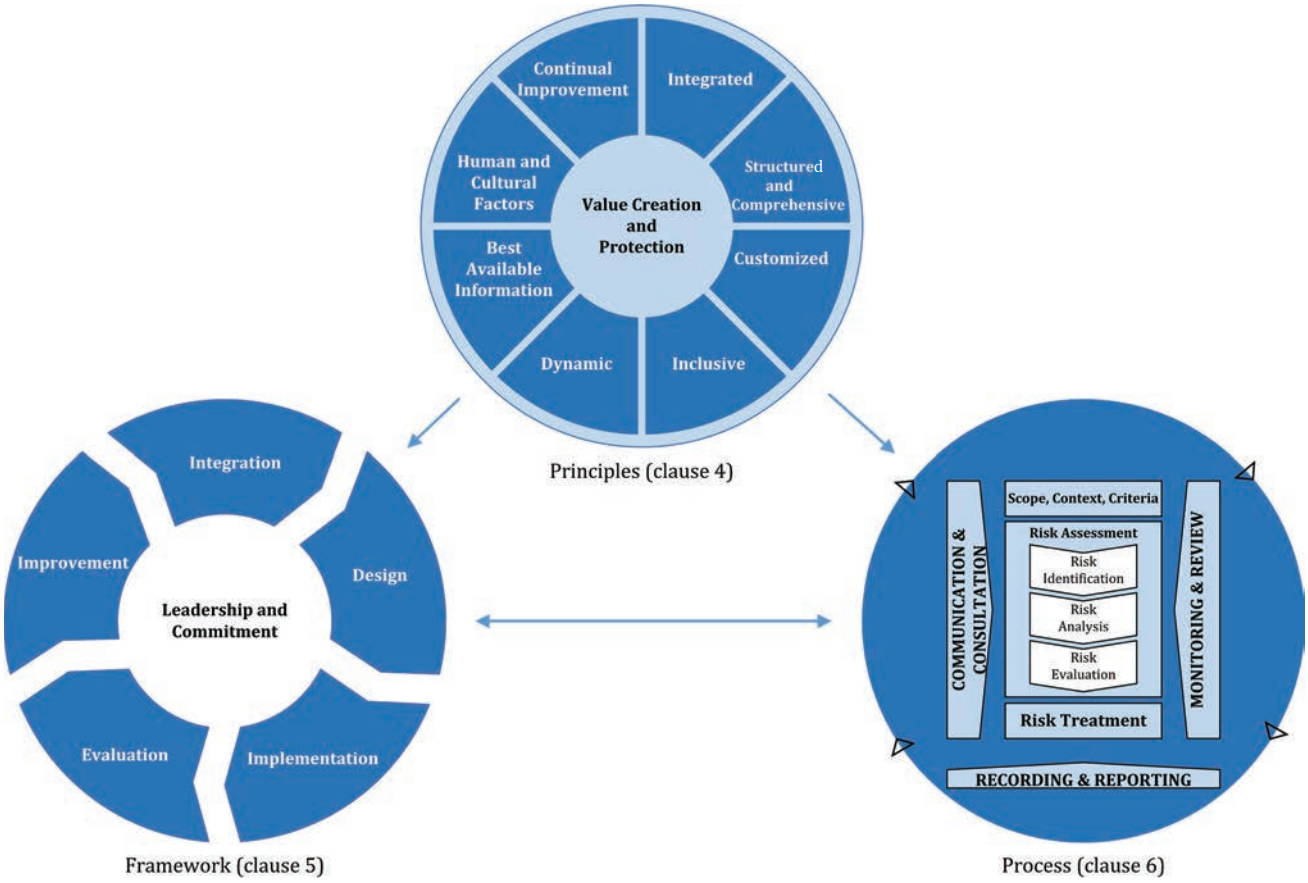


Figure 1 — Principles, framework and process

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.