SVENSK STANDARD
SS-ISO 31000:2018

Riskhantering – Vägledning (ISO 31000:2018, IDT)

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

Svenska Institutet för Standarder

Språk: svenska/Swedish, engelska/English

Utgåva: 2

Svenska Institutet för Standarder

Den här standarden kan hjälpa dig att effektivisera och kvalitetssäkra ditt arbete. SIS har fler tjänster att erbjuda dig för att underlätta tillämpningen av standarder i din verksamhet.

SIS Abonnemang
Snabb och enkel åtkomst till gällande standard med SIS Abonnemang, en prenumerationstjänst genom vilken din organisation får tillgång till all världens standarder, senaste uppdateringarna och där hela din organisation kan ta del av innehållet i prenumerationen.

Utbildning, event och publikationer
Vi erbjuder även utbildningar, rådgivning och event kring våra mest sålda standarder och frågor kopplade till utveckling av standarder. Vi ger också ut handböcker som underlättar ditt arbete med att använda en specifik standard.

Vill du delta i ett standardiseringsprojekt?
Genom att delta som expert i någon av SIS 300 tekniska kommittéer inom CEN (europeisk standardisering) och/eller ISO (internationell standardisering) har du möjlighet att påverka standardiseringsarbetet i frågor som är viktiga för din organisation. Välkommen att kontakta SIS för att få veta mer!

Kontakt
Skriv till kundservice@sis.se, besök sis.se eller ring 08 - 555 523 10

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

Standarden är framtagen av kommittén 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.

Fastställd: 2018-04-05
ICS: 03.100.01;04.050

Svenska Institutet för Standarder

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.

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.

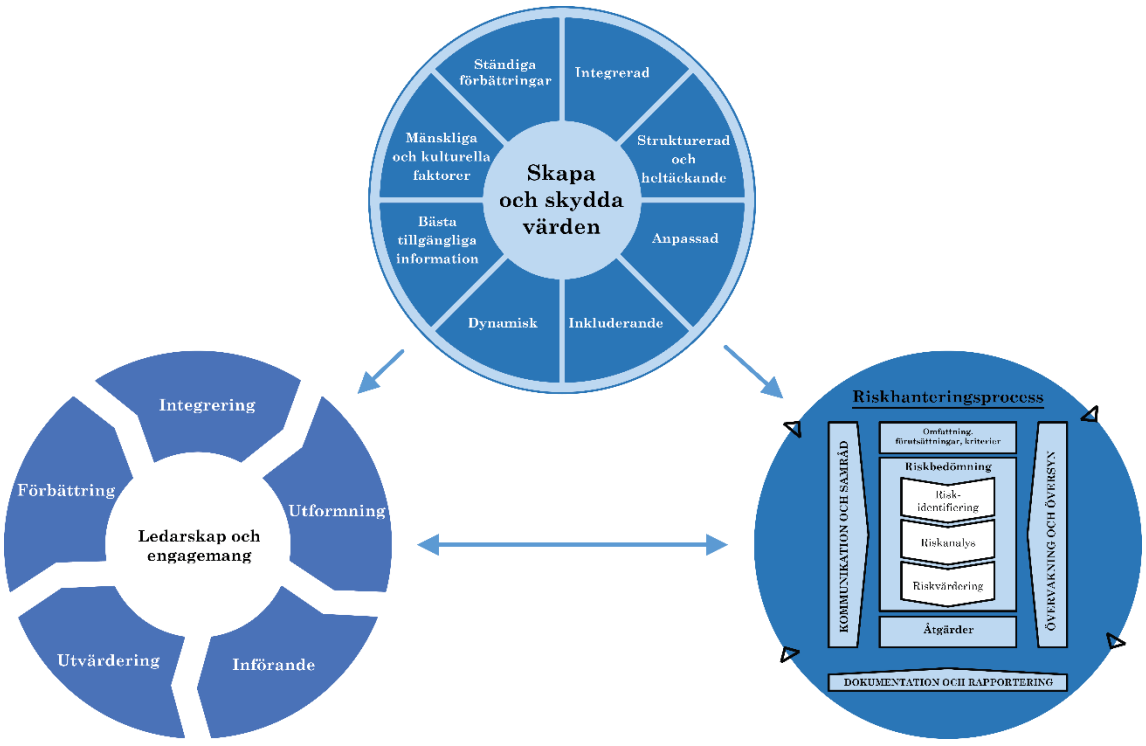
Riskhantering är en iterativ process som hjälper organisationer att fastställa strategier, uppnå mål och fatta välgrundade beslut.

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.

3 Termer och definitioner

För syftena med detta dokument tillämpas följande termer och definitioner.

ISO och IEC har terminologier som kan användas i standardiseringsarbetet och som finns i följande databaser:

– ISO Online Browsing Platform finns på http://www.iso.org/obp

– IEC Electropedia finns på http://www.electropedia.org.

3.1
risk
osäkerhetens effekt på mål

Anm. 1 till termpost: En effekt är en avvikelse från det förväntade. Den kan vara positiv, negativ eller både och. En effekt kan uppstå till följd av en reaktion eller avsaknaden av en respons, på en möjlighet eller ett hot med koppling till målen.

Anm. 2 till termpost: Mål kan ha olika aspekter, ingå i olika kategorier och gälla på olika nivåer.

Anm. 3 till termpost: Risker uttrycks ofta som *riskkällor* (3.4), *potentiella händelser* (3.5), dess *konsekvenser* (3.6) och dess *sannolikhet* (3.7).

3.2
riskhantering
samordnade aktiviteter för att styra och leda en organisation med avseende på *risk* (3.1)

3.3
intressent
person eller organisation som kan påverka, påverkas av eller anse sig bli påverkad av ett beslut eller en aktivitet

Anm. 1 till termpost: Termen ”berörd part” kan användas som ett alternativ till ”intressent”.

3.4
riskkälla
faktor som i sig självt eller i kombination har potential att utgöra en *risk* (3.1)

3.5
händelse
förekomst eller förändring av särskilda omständigheter

Anm. 1 till termpost: En händelse kan vara en eller flera förekomster och kan ha flera orsaker och flera konsekvenser (3.6).

Anm. 2 till termpost: En händelse kan också vara något som förväntas inträffa men som inte inträffar, eller något som inte förväntas inträffa men som inträffar.

Anm. 3 till termpost: En händelse kan vara en riskkälla.

3.6
konsekvens
utfall från en *händelse* (3.5) som påverkar målen

Anm. 1 till termpost: En konsekvens kan vara känd eller oviss och kan ha positiva eller negativa, direkta eller indirekta, effekter på målen.

Anm. 2 till termpost: Konsekvenser kan uttryckas kvalitativt eller kvantitativt.

Anm. 3 till termpost: Direkta konsekvenser kan eskalera genom kaskadeffekter och kumulativa effekter.

3.7
sannolikhet
hur troligt det är att något inträffar

Anm. 1 till termpost: Inom terminologi för *riskhantering* (3.2) används ordet ”sannolikhet” för att benämna hur troligt det är att något inträffar, oavsett om det definieras, mäts eller avgörs objektivt eller subjektivt, kvalitativt eller kvantitativt, eller om det beskrivs i generella termer eller matematiska (såsom en sannolikhet eller frekvens över en viss tidsperiod).

Anm. 2 till termpost: Den engelska termen ”likelihood” har i vissa språk ingen direkt motsvarighet, istället används då vanligen motsvarigheten till termen ”probability”. I engelskan tolkas dock ”probability” som en matematisk term. Därför används termen ”likelihood” inom riskhanteringsterminologin med den vidare tolkningen som ”probability” har i många språk utöver engelskan.

3.8
riskhanteringsåtgärd
åtgärd för att bibehålla och/eller förändra *risker* (3.1)

Anm. 1 till termpost: Riskhanteringsåtgärder omfattar, men är inte begränsade till, processer, policyer, utrustning, rutiner och andra förhållanden och/eller aktiviteter som bibehåller och/eller förändrar risken.

Anm. 2 till termpost: Riskhanteringsåtgärder ger inte alltid den avsedda eller förväntade förändringseffekten.

4 Syfte och principer

Syftet med riskhantering är att skapa och skydda värden. Det förbättrar prestanda, gynnar innovation och stödjer arbetet för att uppfylla mål. Principerna som beskrivs i Figur 2 ger vägledning för effektiv och verkningsfull riskhantering, förmedlar fördelarna och beskriver syftet och ändamålet. Principerna utgör grunden för hantering av risker och de bör beaktas vid utformningen av organisationens ramverk och processer för riskhantering. Dessa principer, som illustreras i Figur 2, bör möjliggöra för organisationer att hantera osäkerhetens effekter på målen.

Figur 2 – **Principer**

Delarna i Figur 2 behövs för verkningsfull riskhantering. Delarna i Figur 2 beskrivs vidare nedan.

a) Integrerad

Riskhantering är en integrerad del av alla organisatoriska aktiviteter.

b) Strukturerad och heltäckande

Ett strukturerat och heltäckande tillvägagångssätt med avseende på riskhantering bidrar till konsekventa och jämförbara resultat.

c) Anpassad

Ramverket och processerna för riskhantering är anpassade och står i proportion till organisationens externa och interna förutsättningar. De är också kopplade till organisationens mål.

d) Inkluderande

Att involvera intressenter på ett lämpligt och tidsanpassat sätt säkerställer att intressenternas kunskaper, synpunkter och åsikter beaktas. Detta ger förbättrade kunskaper och välgrundad riskhantering.

e) Dynamisk

Risker kan uppkomma, förändras eller försvinna när en organisations externa och interna förutsättningar förändras. Riskhantering kan förutse, upptäcka, fastställa och svara på dessa förändringar och händelser på ett lämpligt och tidsanpassat sätt.