SVENSK STANDARD
SS-ISO 31000:2009

Fastställd/Approved: 2009-11-30
Publicerad/Published: 2010-03-30
Utgåva/Edition: 1
Språk/Language: svenska/Swedish
ICS: 03.100.01; 04.050

Riskhantering – Principer och riktlinjer (ISO 31000:2009, IDT)

Risk management – Principles and guidelines (ISO 31000:2009, IDT)

Hitta rätt produkt och ett leveranssätt som passar dig

Standarder
Genom att följa gällande standard både effektiviserar och säkrar du ditt arbete. Många standarder ingår dessutom ofta i paket.

Tjänster
Abonnemang är tjänsten där vi uppdaterar dig med aktuella standarder när förändringar sker på dem du valt att abonnera på. På så sätt är du säker på att du alltid arbetar efter rätt utgåva.
e-nav är vår online-tjänst som ger dig och dina kollegor tillgång till standarder ni valt att abonnera på dygnet runt. Med e-nav kan samma standard användas av flera personer samtidigt.

Leveranssätt
Du väljer hur du vill ha dina standarder levererade. Vi kan erbjuda dig dem på papper och som pdf.

Andra produkter
Vi har böcker som underlättar arbetet att följa en standard. Med våra böcker får du ökad förståelse för hur standarder ska följas och vilka fördelar den ger dig i ditt arbete. Vi tar fram många egna publikationer och fungerar även som återförsäljare. Det gör att du hos oss kan hitta över 500 unika titlar. Vi har även tekniska rapporter, specifikationer och "workshop agreement". Matriser är en översikt på standarder och handböcker som bör läsas tillsammans. De finns på sis.se och ger dig en bra bild över hur olika produkter hör ihop.

Standardiseringsprojekt
Du kan påverka innehållet i framtida standarder genom att delta i någon av SIS ca 400 Tekniska Kommittéer.

Find the right product and the type of delivery that suits you

Standards
By complying with current standards, you can make your work more efficient and ensure reliability. Also, several of the standards are often supplied in packages.

Services
Subscription is the service that keeps you up to date with current standards when changes occur in the ones you have chosen to subscribe to. This ensures that you are always working with the right edition.
e-nav is our online service that gives you and your colleagues access to the standards you subscribe to 24 hours a day. With e-nav, the same standards can be used by several people at once.

Type of delivery
You choose how you want your standards delivered. We can supply them both on paper and as PDF files.

Other products
We have books that facilitate standards compliance. They make it easier to understand how compliance works and how this benefits you in your operation. We produce many publications of our own, and also act as retailers. This means that we have more than 500 unique titles for you to choose from. We also have technical reports, specifications and workshop agreements. Matrices, listed at sis.se, provide an overview of which publications belong together.

Standardisation project
You can influence the content of future standards by taking part in one or other of SIS's 400 or so Technical Committees.

Den internationella standarden ISO 31000:2009 gäller som svensk standard. Standarden fastställdes 2009-11-30 som SS-ISO 31000:2009 och har utgivits i engelsk språkversion. Detta dokument återger ISO 31000:2009 i svensk språkversion. De båda språkversionerna gäller parallellt.

The International Standard ISO 31000:2009 has the status of a Swedish Standard. The standard was 2009-11-30 approved and published as SS-ISO 31000:2009 in English. This document contains a Swedish language version of ISO 31000:2009. The two versions are valid in parallel.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00.
Standarder kan beställas hos SIS Förlag AB 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), tel +46 8 555 520 00.
Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

SIS Förlag AB, SE 118 80 Stockholm, Sweden. Tel: +46 8 555 523 10. Fax: +46 8 555 523 11.
E-mail: sis.sales@sis.se Internet: www.sis.se

Innehåll

Sida

Förord ... **iii**

Orientering ... **iv**

1 Omfattning ... **1**

2 Termer och definitioner ... **1**

3 Principer ... **7**

4 Ramverk ... **8**
4.1 Allmänt ... 8
4.2 Mandat och åtagande ... 9
4.3 Utformning av ramverk för hantering av risker ... 10
4.3.1 Förstå organisationen och dess kontext ... 10
4.3.2 Upprätta policy för riskhantering ... 10
4.3.3 Ansvar ... 11
4.3.4 Integrering i organisatoriska processer ... 11
4.3.5 Resurser ... 11
4.3.6 Upprätta intern kommunikation och rapporteringsmetoder ... 12
4.3.7 Upprätta extern kommunikation och rapporteringsmetoder ... 12
4.4 Implementering av riskhantering ... 12
4.4.1 Implementera ramverket för hantering av risker ... 12
4.4.2 Implementera riskhanteringsprocessen ... 13
4.5 Övervakning och granskning av ramverket ... 13
4.6 Kontinuerlig förbättring av ramverket ... 13

5 Process ... **13**
5.1 Allmänt ... 13
5.2 Kommunikation och konsultation ... 14
5.3 Etablering av kontexten ... 15
5.3.1 Allmänt ... 15
5.3.2 Etablering av den externa kontexten ... 15
5.3.3 Etablering av den interna kontexten ... 15
5.3.4 Etablering av kontexten för riskhanteringsprocessen ... 16
5.3.5 Definiering av riskkriterier ... 17
5.4 Riskbedömning ... 17
5.4.1 Allmänt ... 17
5.4.2 Riskidentifiering ... 17
5.4.3 Riskanalys ... 18
5.4.4 Riskutvärdering ... 18
5.5 Riskbehandling ... 18
5.5.1 Allmänt ... 18
5.5.2 Val av riskbehandlingsalternativ ... 19
5.5.3 Dokumentera riskhanteringsprocessen ... 20
5.6 Övervakning och granskning ... 20
5.7 Dokumentera riskhanteringsprocessen ... 21

Bilaga A (informativ) Attribut för utvecklad riskhantering ... **22**

Litteraturförteckning ... **24**

Förord

ISO (Internationella standardiseringsorganisationen) är ett internationellt standardiseringsorgan (ISO-medlemsorgan). Arbetet med att förbereda internationella standarder utförs normalt via ISOs tekniska kommittéer. Alla medlemsorgan som är intresserade av ett ämne det finns en teknisk kommitté för har rätt att representeras i den kommittén. Andra internationella organisationer, statliga eller privata, som samarbetar med ISO och IEC, deltar också i arbetet. ISO har ett nära samarbete med internationella elektrotekniska kommissionen (IEC) i alla ärenden som rör elektroteknisk standardisering.

Internationella standarder utformas i enlighet med de regler som anges i ISO/IEC-direktiven, del 2.

De tekniska kommittéernas huvudsakliga uppgift är att förbereda internationella standarder. Förslag till internationella standarder från de tekniska kommittéerna cirkuleras hos medlemsorganen för omröstning. Publicering som en internationell standard kräver godkännande av minst 75 % av de medlemsorgan som röstar.

Det bör framhållas att vissa delar av detta dokument kan omfattas av patenträttigheter. ISO ska inte hållas ansvarig för identifiering av sådana patenträttigheter.

ISO 31000 har utarbetats av ISO Technical Management Board Working Group on risk management.

Orientering

Organisationer av alla typer och storlekar ställs inför både interna och externa faktorer och influenser som bidrar till osäkerhet gällande om och när de kommer att uppnå sina mål. Den effekt denna osäkerhet har på en organisations mål är en ”risk”.

Alla aktiviteter inom en organisation medför risker. Organisationer hanterar risker genom att identifiera och analysera dem och därefter utvärdera om risken ska modifieras genom riskbehandling för att uppfylla organisationens riskkriterier. Under denna process kommunicerar och konsulterar organisationen med intressenter, och övervakar och granskar de risker och kontroller som förändrar risken för att säkerställa att ingen ytterligare riskbehandling krävs. Denna internationella standard beskriver denna systematiska och logiska process i detalj.

Medan alla organisationer i någon utsträckning hanterar risker, fastställer denna internationella standard ett antal principer som behöver uppfyllas för att göra riskhanteringen effektiv. Denna internationella standard rekommenderar att organisationer utformar, implementerar och fortlöpande förbättrar ett ramverk vars syfte är att integrera riskhanteringsprocessen i organisationens övergripande styrning, strategi och planering, ledning, rapporteringsprocesser, policyer, normer och kultur.

Riskhantering kan tillämpas på en hel organisation, på dess olika områden och nivåer, när som helst och på specifika funktioner, projekt och aktiviteter.

Även om användning av riskhantering har utvecklats över tid och inom många sektorer för att motsvara olika behov, kan tillämpning av konsekventa processer inom ett heltäckande ramverk bidra till att säkerställa att risker hanteras effektivt, ändamålsenligt och samstämmigt genom en organisation. Det allmänna tillvägagångssätt som beskrivs i denna internationella standard tillhandahåller principer och riktlinjer, för hantering av vilken sorts risk som helst, på ett systematiskt, tydligt och trovärdigt sätt och inom vilken omfattning och kontext som helst.

Varje specifik sektor eller riskhanteringsapplikation medför individuella behov, mottagare, uppfattningar och kriterier. Därför omfattar denna internationella standard ett huvudmoment som inbegriper ”etablering av kontext” som en aktivitet vid start av den generella riskhanteringsprocessen. Genom att etablera kontexten insamlas organisationens mål, omgivningen i vilken målen ska eftersträvas, dess intressenter och riskkriteriernas mångfald – vilket sammantaget är behjälpligt för att uppdaga och bedöma karaktären och komplexiteten hos dess risker.

Relationen mellan principerna för hantering av risk, ramverket inom vilket hanteringen förekommer och de riskhanteringsprocesser som beskrivs i denna standard visas i figur 1.

Riskhantering, om implementerad och underhållen enligt denna internationella standard, möjliggör för organisationen att exempelvis:

— öka sannolikheten för att uppnå målen

— uppmuntra till proaktiv styrning

— bli medveten om behovet av att identifiera och behandla risker genom organisationen

— förbättra möjligheten att identifiera möjligheter och hot

— följa relevanta lagliga och reglerande krav och internationella standarder

— förbättra obligatorisk och frivillig rapportering

— förbättra styrning

— öka intressenternas förtroende och tillit

— etablera en tillförlitlig grund för beslutsfattande och planering

— förbättra kontroller

— effektivt tilldela och använda resurser för riskhantering

— förbättra driftens effektivitet och ändamålsenlighet

— förbättra såväl hälsa och säkerhetsprestanda, som miljöskydd

— främja förebyggande av förluster och incidenthantering

— minimera förluster

— förbättra organisatorisk utbildning

— förbättra organisatorisk återhämtningsförmåga.

Denna internationella standard är avsedd att möta en mängd olika intressenters behov inklusive:

a) de som ansvarar för utformning av riskhanteringspolicy inom sin organisation

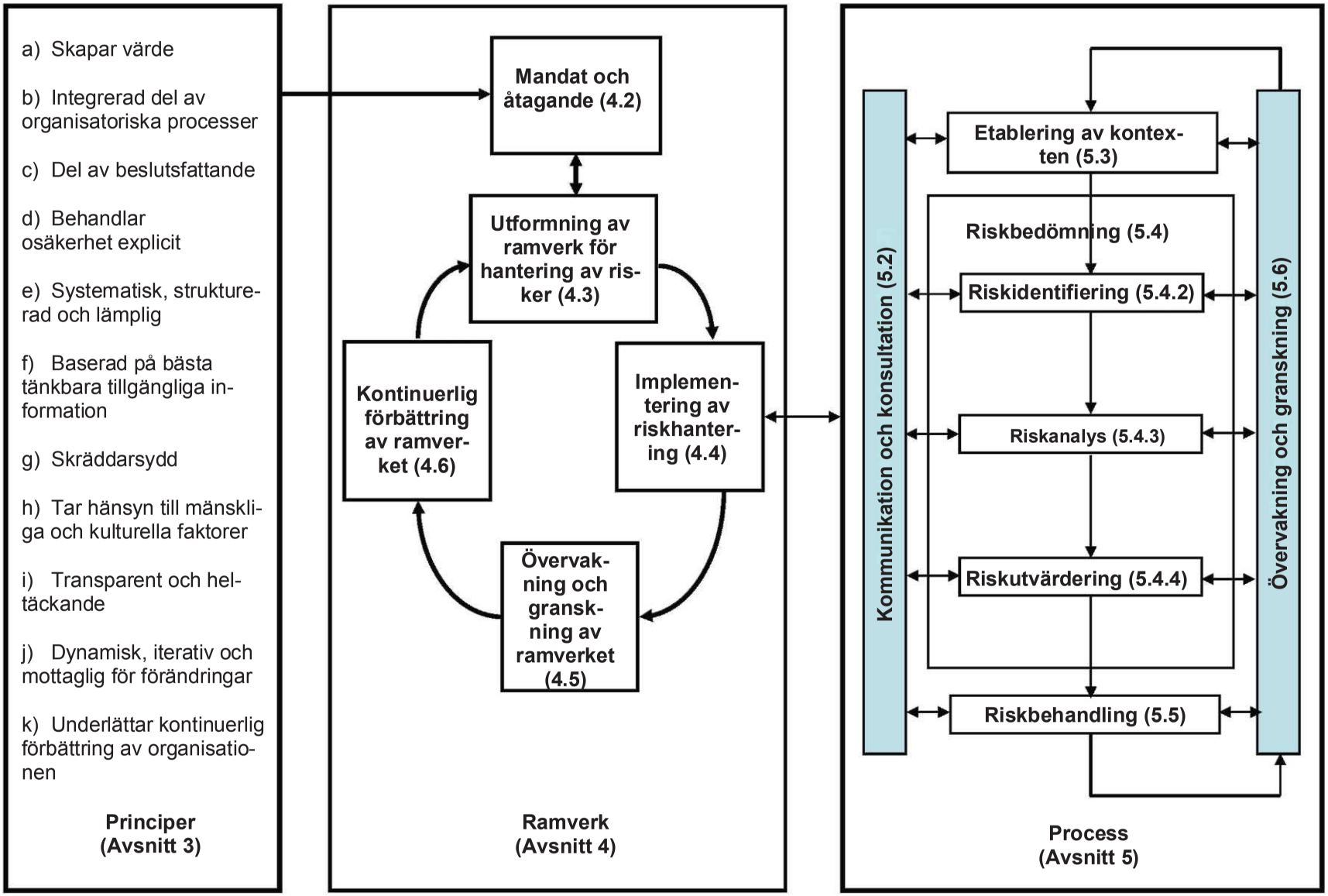
b) de som ansvarar för att säkerställa att risker hanteras inom hela organisationen eller inom en/ett specifik(t) område, projekt eller aktivitet

c) de som ska utvärdera en organisations riskhanteringseffektivitet

d) utvecklare av standarder, vägledningar, rutiner och riktlinjer som, helt eller delvis, anger hur risker ska hanteras inom dessa dokuments specifika kontext.

Många organisationers befintliga metoder och processer för styrning inkluderar riskhanteringskomponenter och många organisationer har redan antagit en formell riskhanteringsprocess för särskilda typer av risker eller omständigheter. I sådana fall kan en organisation bestämma sig för att genomföra en kritisk granskning av befintliga metoder och processer i ljuset av denna internationella standard.

I denna internationella standard används både uttrycket ”riskhantering” och ”hantering av risker”. I generella ordalag avser ”riskhantering” arkitekturen (principer, ramverk och processer) för att hantera risker effektivt, medan ”hantering av risker” avser tillämpning av den arkitekturen på särskilda risker.



Figur 1 – Relationer mellan riskhanteringsprinciper, ramverk och process

Riskhantering – Principer och riktlinjer

1 Omfattning

Denna internationella standard tillhandahåller principer och generella riktlinjer för riskhantering.

Denna internationella standard kan användas av offentliga, privata eller kommunala verksamheter, organisationer, grupper eller individer. Denna internationella standard är därför inte bransch- eller sektorspecifik.

ANM. För enkelhetens skull benämns alla användare av denna standard med den allmänna termen ”organisation”.

Denna internationella standard kan tillämpas under en organisations hela livslängd på ett flertal olika aktiviteter, inklusive strategier och beslut, drift, processer, funktioner, projekt, produkter, tjänster och tillgångar.

Denna internationella standard kan tillämpas på alla sorters risker, oavsett karaktär, och oavsett om de har positiva eller negativa konsekvenser.

Även om denna internationella standard ger allmänna riktlinjer är den inte avsedd att skapa likadan riskhantering i alla organisationer. Vid utformning och implementering av riskhanteringsplaner och ramverk bör hänsyn tas till varierande behov hos en specifik organisation, dess särskilda mål, kontext, struktur, drift, processer, funktioner, projekt, produkter, tjänster, tillgångar och särskilda rutiner.

Avsikten är att denna internationella standard ska användas för att harmonisera riskhanteringsprocesser i befintliga och kommande standarder. Den tillhandahåller ett gemensamt tillvägagångssätt till stöd för standarder som behandlar särskilda risker och/eller sektorer, och ersätter inte de standarderna.

Denna internationella standard är inte ämnad för certifiering.