

ferma



FEDERATION OF
EUROPEAN RISK
MANAGEMENT
ASSOCIATIONS

STANDARD FÖR RISK MANAGEMENT





Inledning

Denna standard för riskhantering är resultatet av arbete som utförts av ett team från de ledande intresseorganisationerna för riskhantering i Storbritannien

- IRM (The Institute of Risk Management)
- AIRMIC (The Association of Insurance and Risk Managers)
- ALARM (The National Forum for Risk Management in the Public Sector).

Teamet har tagit hänsyn till uppfattningar och synpunkter som lämnats av andra professionella organisationer inom riskhantering.

Riskhantering är ett ämne som utvecklats snabbt och synen på denna verksamhet och dess mål varierar starkt. Det bör finnas en standard för att underlätta kommunikationen och skapa en samsyn. Standarden bör främst ta sikte på riskhanterings

- *begrepp*
- *processer*
- *organisation*
- *mål*

Riskhantering är i grunden en fråga om att hantera osäkerheter. Det är viktigt att standarden tar hänsyn till att risktagande har både en positiv och en negativ sida. Med detta menas att risktagande är ett oundvikligt element i all verksamhet och i all utveckling. De möjligheter som ligger i risktagande kan behandlas med liknande metodik som de förluster som kan uppkomma.

Riskhantering är viktigt för både näringsliv och offentlig sektor och egentligen för alla organisationer och verksamheter, både på kort och på lång sikt.

Nyttan och värdet av riskhantering ska ses i ett helhetsperspektiv som omfattar en organisation, dess verksamheter och alla dess intressenter.

Formerna och verktygen för riskhantering skiljer sig mellan olika organisationer och verksamheter. Det går inte i en standard att beskriva riskhantering i detalj. Standarden beskriver övergripande syfte, struktur, mål och processer. Genom att uppfylla denna standard kommer olika organisationer, låt vara på skilda sätt, att kunna deklarerera att de lever upp till god praxis inom riskhantering.

Standarden har så långt möjligt använt den terminologi för riskhantering som är avsedd för standarder enligt dokumentet ISO/IEC Guide 73 (Risk Management - Vocabulary - Guidelines for use in standards) utgiven av ISO (International Organization for Standardization).

Mot bakgrund av den snabba utvecklingen inom det här området är författarna tacksamma för synpunkter från de organisationer som inför denna standard. Avsikten är att anpassa standarden till verkligheten på bästa sätt enligt beprövad erfarenhet och kunskap. Denna svenska översättning har gjorts i regi av Swedish Risk Management Association, SWERMA. Kontakt med SWERMA kan ske via info@swerma.se eller www.swerma.se.



1. Risk

Risk kan definieras som kombinationen av sannolikheten för en viss händelse och dess konsekvenser (ISO/IEC Guide 73).

Verksamheter av alla de slag och deras framgång kan påverkas av händelser och omständigheter som innebär möjlighet eller hot.

Riskhantering blir i allt större utsträckning en fråga om att se både de positiva och negativa perspektiven av risktagande. Därför behandlar denna standard risktagande ur båda perspektiven.

Traditionell riskhantering å andra sidan inriktar sig i allmänhet enbart på vissa kategorier av skadehändelser samt försäkringsbara risker. Liknande gäller för myndigheter och andra organisationer med uppgift att svara för skapande av regelverk, övervakning och tillsyn, planering, beredskap samt skydd och säkerhet för människor och samhället med dess funktioner.

2. Riskhantering

Riskhantering är en central del av den strategiska styrningen av varje organisation. Det är den process som organisationer använder sig av för att uppnå en systematisk hantering av sina risker. Målet ska vara att uppnå kort- och långsiktig nytta både för varje enskild aktivitet och för helheten. Därmed ökar samtidigt säkerheten för att organisationens övergripande mål kan uppnås.

Identifiering av riskerna är grunden för all riskhantering.

Riskhantering

- ska vara en kontinuerlig och framåtriktad process i organisationens hela strategi och förverkligandet av denna.
- ska metodiskt ta tag i alla risker som är förknippade med organisationen och dess verksamhet i förfluten tid, nutid och framtid.
- ska vara en del av organisationens kultur med en klart uttalad policy och ett program som företagsledningen ställer sig bakom.

Ansvaret för riskhantering ska delegeras till chefer och anställda. Detta ska framgå av deras arbetsbeskrivning.

Genomförandet bör stödjas genom resultat- eller rapporteringsansvar, prestationsmätningar och belöningsystem som främjar den operativa effektiviteten på alla nivåer.

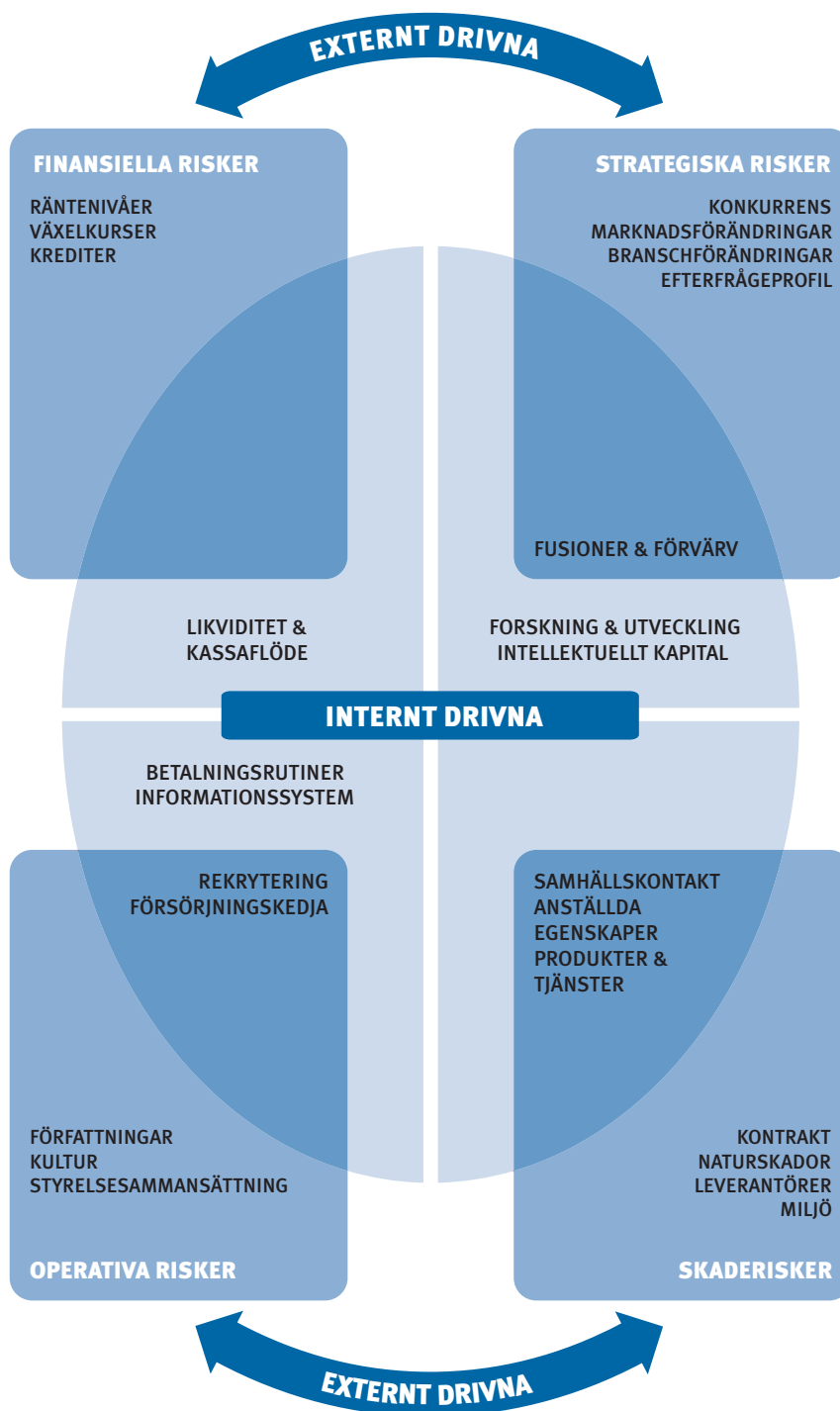
2.1 Externa och interna faktorer

De risker som en organisation och dess operativa enheter utsätts för kan bero på både externa och interna faktorer.

Figuren på nästa sida ger exempel på väsentliga risker med hänsyn till både externa och interna drivkrafter. De två perspektiven kan alltså överlappa varandra. Riskerna kan vidare delas in i risktyper som t.ex. strategiska risker, finansiella risker, operativa risker, skaderisker etc.

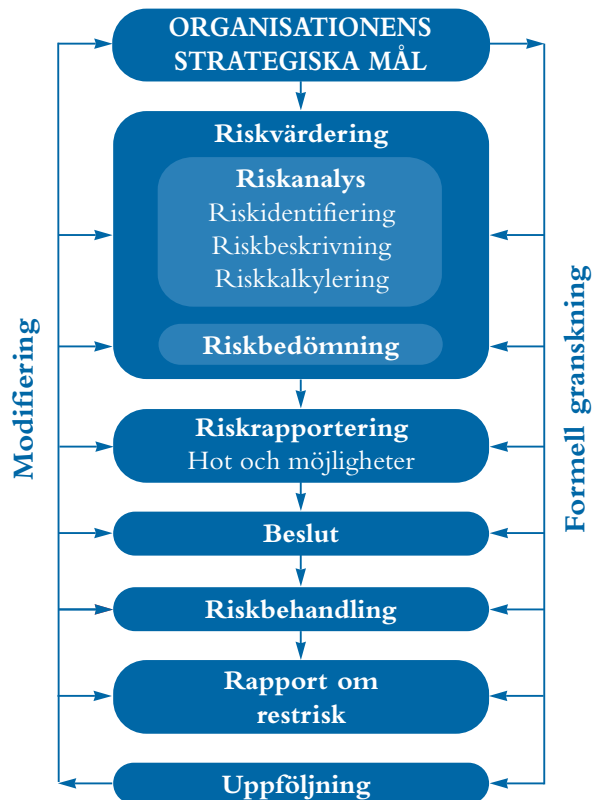


2.1 Exempel på källor till väsentliga risker





2.2 Riskhanteringsprocessen



Riskhantering skapar mervärde för en organisation och dess intressenter och bidrar till att verksamheten når sina mål och planer genom att:

- vara ett verktyg när det gäller att utveckla ny verksamhet och att hantera förekommande osäkerhet på ett systematiskt och konsekvent sätt
- förbättra beslutsfattande, planering och prioritering genom grundlig insikt rörande förutsättningar, hot, möjligheter och känslighet i verksamhet och projekt
- bidra till mer effektiv användning av kapital och resurser
- minska risknivån utanför kärnverksamheten
- skydda och förstärka ställning, förtroende och image
- utveckla och stödja personer och organisationens kunskapsbas
- effektivisera verksamheten



3. Riskvärdering

Riskvärdering definieras av ISO/IEC Guide 73 som den övergripande processen med riskanalys och riskbedömning som innefattar alla påverkande faktorer i samband med riskhantering, d.v.s. ett antal faktorer som riskaversion, osäkerheter, attityder, psykologiska, strategiska, taktiska, politiska faktorer etc. Riskvärdering och riskbedömning har både kvantitativa och kvalitativa inslag och påverkas, i synnerhet i de kvalitativa delarna, av kulturella bakgrunder, önsknings, attityder och idéer.

4. Riskanalys

4.1 Riskidentifiering

Riskidentifiering avser att upptäcka och tydliggöra alla risker en organisation är utsatt för. De ska beskrivas, registreras och kategoriseras. Organisationens känslighet för olika risker i termer av både orsaker och konsekvenser är en viktig utgångspunkt för att identifiera och kategorisera. Risker ska identifieras i fråga om t.ex. både verksamhet och beslut. Riskidentifiering är en i huvudsak kvalitativ process där olika möjliga händelsers orsaker, konsekvenser och sambanden dem emellan kartläggs.

Detta kräver ingående kunskap om organisationen, den marknad där organisationen arbetar, dess juridiska, sociala, politiska och kulturella miljö och en utvecklad medvetenhet om dess strategiska mål och verksamhetsmål inklusive kritiska framgångsfaktorer samt de hot och möjligheter som har betydelse för att dessa mål ska uppnås.

Riskidentifiering ska utföras på ett metodiskt sätt för att alla betydande riskkällor och riskfaktorer inom organisationen ska kunna identifieras.

Risker kan kategoriseras mot en bakgrund av verksamhet och beslut på ett antal sätt, t.ex. enligt följande:

- *Strategiska* - Dessa hänför sig till en organisations långsiktiga strategiska målsättningar. De kan påverkas av sådana faktorer som tillgång till kapital, politiska beslut, ändring av lagstiftning och regelverk, förtroende, anseende samt förändringar i omvärlden.
- *Taktiska* - Dessa hänför sig till vilka vägar och lösningar en organisations valt för att uppnå de strategiska målen.
- *Operativa* - Dessa hänför sig till de dagliga uppgifter som en organisation har att lösa när den strävar efter att nå sina verksamhetsmål, taktiska och strategiska mål.
- *Ekonomiska* - Dessa hänför sig till en organisations ekonomistyrning och påverkan från externa faktorer som t. ex. tillgången på krediter, valutakurser, förändringar i ränteläge, kapitalförvaltning etc.
- *Kunskap och information* - Dessa hänför sig till kunskapsresurser, produktion, verksamhetsskydd samt kommunikation och informationshantering.
- *Efterlevnad* - Dessa hänför sig till regelverk på olika områden som hälsa och säkerhet, miljöfrågor, produkt- och verksamhetsbeskrivningar, konsumentskydd, dataskydd, rekryteringsrutiner, författningar etc.
- *Projektrelaterade* - Dessa hänför sig till alla aktiviteter och uppgifter som utförs i projektform, oavsett på vilken nivå eller med vilket syfte projektet har skapats.
- *Processrelaterade* - Dessa hänför sig till alla de processer som organisationen arbetar efter oavsett nivå eller syfte.

Riskidentifiering kan visserligen utföras av externa konsulter men ett internt angreppssätt med väl förankrade, systematiska och samordnade processer och verktyg (se Bilaga) är sannolikt mera effektiv. Det är väsentligt att riskhanteringsprocessen "ägs" internt.



4.2 Beskrivning

De identifierade riskerna bör beskrivas på ett kortfattat, begripligt och strukturerat sätt. Att använda en väl utformad struktur är nödvändigt för att säkerställa en sammanhängande process för identifiering, beskrivning och värdering av risker. Tabell 4.2.1 är ett exempel som kan användas för att presentera risker i en kompakt form.

Genom att grovt skatta konsekvensen och sannolikheten för var och en av riskerna kan man rangordna riskerna med hänsyn till hur allvarliga de är och ta fram dem som behöver analyseras mer i detalj.

Det är viktigt att riskhantering för varje projekt påbörjas redan på idé- och planeringsstadierna och sedan pågår genom dess hela löptid.

4.2.1 Tabell - Riskbeskrivning

1. Riskens namn/beteckning	
2. Riskområde	Beskrivning av händelserna, storlek, beroenden mm
3. Riskkategori	Exv. strategiska, operativa, ekonomiska/finansiella, kunskaps- eller efterlevnadsrisker
4. Intressenter	Intressenterna och deras förväntningar
5. Kvantifiering	Påverkan och sannolikhetsbedömning
6. Känslighet/tolerans	Potentiell förlust eller ekonomisk påverkan Värden under risk Sannolikhet och storlek på potentiell förlust/vinning
7. Riskhanteringsåtgärder	Uppsatta mål för åtgärderna, önskat resultat Redan genomförda riskhanteringsåtgärder Tilltro till processer, åtgärder och uppföljning
8. Möjliga förbättringar	Rekommendationer för att begränsa verksamhetens risker
9. Utveckling av policy/riskstrategier	Ansvarig person för utveckling/utförande av policy och strategier för riskhantering

4.3 Kalkylering

Risker kan kalkyleras mer eller mindre precist och noggrant. Kalkyler handlar om kvantitativa metoder. En överslagskalkyl kan kallas för en skattning.

En översiktlig värdering som i huvudsak är kvalitativ kan vi kalla för en bedömning. Det kan vara så att det saknas kvantitativa data eller helt enkelt rör sig om attityder till vissa fenomen.

T.ex. kan konsekvensen av både hot (negativ sida av risktagandet) och möjligheter (positiv sida av risktagandet) benämnas hög, medelhög eller låg (se tabell 4.3.1). Sannolikheten kan

också benämnas hög, medelhög eller låg men båda kan behöva kalibreras olika, även avseende på hot resp. möjligheter (se tabellerna 4.3.2 och 4.3.3).

Olika organisationer kommer att upptäcka att man behöver använda olika storheter eller faktorer för konsekvenser och sannolikhet så som passar just för dem.

Många organisationer finner att det ofta räcker att bedöma konsekvenser och sannolikhet i nivåerna hög, medelhög eller låg, varvid resultaten kan presenteras som en 3 x 3 matris. Andra organisationer kan behöva analysera konsekvenser och sannolikhet med hjälp av en



5 x 5-matris, vilket vid behov kan ge dem en mer nyanserad värdering. Antalet nivåer styrs av vilken upplösning man behöver. Högre upplösning än vad en 10 x 10 matris ger torde inte behövas.

Om en matris ska användas som skattningar av absoluta utfall måste axlarna graderas på motsvarande sätt, t.ex. frekvens i ggr per år och konsekvens i pengar.

Table 4.3.1 Bedömning av påverkan – risker och möjligheter/ möjlig förlust/vinst

Hög	Ekonomiskt utfall överstiger sannolikt Y kr Betydande påverkan på verksamheten och möjligheten att genomföra valda strategier Väcker betydande uppmärksamhet hos verksamhetens intressenter
Medel	Ekonomiskt utfall beräknas ligga i intervallet X kr – Y kr Icke ringa påverkan på verksamhet och möjligheten att genomföra valda strategier Väcker viss uppmärksamhet hos verksamhetens intressenter
Låg	Ekonomiskt utfall beräknas understiga X kr. Ringa påverkan på verksamhet och möjligheten att genomföra valda strategier Ringa eller ingen uppmärksamhet hos verksamhetens intressenter

Table 4.3.2 Bedömning av frekvens-/sannolikhet - fara/förlust

Bedömning	Mått	Indikation
Hög	Kan inträffa i genomsnitt 1 gång årligen. Sannolikhet > 25%.	Finns statistik för frekvensen. Inträffar minst en gång av 4 möjliga fall.
Medel	Kan inträffa i genomsnitt 1 gång på 10-år. Sannolikhet < 25%.	Finns statistik för frekvensen. Inträffar minst en gång av 4 möjliga fall.
Låg	Inträffar i genomsnitt mindre än en gång på 10 år. Sannolikhet < 2%.	Tillgänglig branschfarenhet. Inträffar mindre än en gång av 50 möjliga fall.



Table 4.3.3 Bedömning av frekvens/sannolikhet - möjlighet/vinst

Bedömning	Mått	Indikator
Hög	Gynnsamt utfall uppnås sannolikt inom ett år. Chans > 75%.	Uppenbar möjlighet som kan utnyttjas med rimlig grad av visshet. Kan uppnås på kort sikt med stöd av befintliga ledningsresurser. Gynnsamt utfall i mer än 3 fall av 4.
Medel	Rimliga möjligheter att uppnå gynnsamt utfall inom ett år. Chans mellan 25% och 75%.	Möjligheter som skulle kunna realiseras men som kräver särskild ledning. Möjligheter som skulle kunna innebära att mål och planer överträffas. Gynnsamt utfall i mellan 1 och 3 fall av 4.
Låg	Gynnsamt utfall kan kanske uppnås på medellång sikt. Chans < 25 %.	Möjlighet som återstår att till fullo analysera. Möjlighet som inte har så stor chans att leda till framgång p.g.a. rådande brist på ledningsresurser. Gynnsamt utfall i högst 1 fall av 4.

4.4 Riskanalysmetodik, metoder och tekniker

Det finns en grundläggande metodik för att analysera risker. På denna bas har det utvecklats ett antal metoder och tekniker för olika tillämpningar. Dessa kan skilja sig åt mellan risktagandets positiva eller negativa sida, eller avse både och. (Se *Bilaga*).

4.5 Riskprofil

Resultatet från riskanalysen kan användas till att skapa en riskprofil. Den ger ett verktyg för att prioritera åtgärder för riskbehandling. En

riskprofil som tas fram på ett entydigt sätt för en hel organisation sammanfattar och presenterar på ett lättillgängligt sätt riskerna rangordnade efter hur allvarliga de är. En risk kan hänföras till det verksamhetsområde som påverkas. Man kan också beskriva befintliga åtgärder och indikera var nivån på skyddsinsatser bör ökas, minskas eller omfördelas.

Tydlig ansvarsfördelning bidrar till att klargöra vem som "äger" risken och att den ägnas tillräcklig uppmärksamhet från ledningens sida.



5. Riskbedömning

Sista steget i riskanalysen är att jämföra riskerna med de acceptanskriterier som organisationen fastslagit. Acceptanskriterierna kan gälla risk eller säkerhet och uttryckas i nyttokostnad, lagkrav, socioekonomiska och miljömässiga faktorer, betydelse för intressenterna etc. Genom riskbedömningen ska man komma fram till en gemensam uppfattning av hur allvarliga de risker är som påverkar organisationen och för varje enskild risk ta beslut om den ska accepteras eller åtgärdas.

6. Riskbehandling

Riskbehandling är den process där man väljer och genomför åtgärder för att påverka risken. Syftet är att styra eller begränsa risken, vilket i sig omfattar flera olika möjligheter, t.ex. undvikande, risköverföring, riskfinansiering etc.

OBS: I den här standarden avser riskfinansiering olika lösningar (t.ex. försäkring) som finns för att hantera finansiella eller ekonomiska risker. Riskfinansiering anses normalt inte innefatta finansiering av åtgärder för riskbehandling (enligt definitionen i ISO/IEC Guide 73, se sid. 17).

Ett system för riskbehandling bör förväntas resultera i förbättringar i fråga om:

- organisationens effektivitet
- intern kontroll
- efterlevnad av lagar och förordningar

Riskanalysen bidrar till en effektivt fungerande organisation genom att identifiera de risker som kräver uppmärksamhet från ledningen. Det kommer an på ledningen att prioritera åtgärder för att behandla risker alltefter den nytta det kan medföra för organisationen.

Effektiviteten i riskbehandlingen uttrycks i termer av om risken kommer att elimineras eller i vilken grad den minskar genom de föreslagna åtgärderna.

Kostnadseffektiviteten i riskbehandlingen uttrycks genom kostnaden för en åtgärd jämfört med den förväntade nyttan av en minskad risk.

Kostnaderna för en föreslagen åtgärd behöver ställas i relation till den möjliga ekonomiska konsekvensen om ingen åtgärd vidtas. Detta kräver nästan alltid att mer detaljerade underlag tas fram än vad som finns från början.

Först och främst måste kostnaden för genomförandet utredas. Den måste kalkyleras med viss noggrannhet eftersom den blir det mått mot vilket kostnadseffektiviteten mäts. Den förlust som kan förväntas om ingen åtgärd vidtas måste också kalkyleras. Genom att jämföra de två resultaten kan ledningen avgöra om en åtgärd ska genomföras.

Författningar och regelverk måste efterlevas. En organisation måste ha kunskap om dessa och ett system som säkerställer efterlevnaden. Det är bara i vissa fall som det finns ett visst utrymme för egna avgöranden om det kanske inte finns någon som helst proportionalitet mellan kostnad och risk. Det kan dock finnas andra konsekvenser, t.ex. i fråga om gott rykte eller förtroende, som gör att en organisation som en god samhällsaktör inte åsidosätter efterlevnaden.

Riskfinansiering, vanligen då försäkring, kan ta hand om finansiella aspekter. Man bör dock komma ihåg dels att alla risker eller kostnader inte går att försäkra, dels att förtroendet eller anseendet ändå kan förloras på marknaden eller i samhället. Det kan leda till stora påfrestningar, t.ex. ledningsproblem, minskat börsvärde, köpmotstånd, mediauppmärksamhet, kriser, försämrad position, psykisk ohälsa, sämre moral och minskad lojalitet hos anställda etc.



7. Rapportering och kommunikation

7.1 Intern rapportering

Olika nivåer och enheter inom en organisation behöver olika slags information med olika syften och för olika ändamål från organisationens egen riskhanteringsprocess.

Styrelsen bör:

- veta vilka de allvarligaste riskerna är, som organisationen är utsatt för
- vara medveten om vilken påverkan olika händelser kan medföra uttryckt i t.ex. marknadsvärde, avvikelser i förhållande till förväntade resultat eller avbrott i verksamheten
- se till att erforderligt risk- och säkerhetsmedvetande finns i hela organisationen
- kunna lita på att organisationen kan hantera en kris
- förstå hur olika intressenters förtroende för organisationen påverkas av olika händelser
- styra informationen till intressenterna, t.ex. aktieägarna, aktiemarknaden, media eller allmänheten
- kunna känna sig säkra på att organisationens riskhantering fungerar effektivt
- initiera att organisationen ger ut en tydlig policy för riskhantering, som omfattar riskhanteringsfilosofi och ansvarsförhållanden

Verksamhets- eller resultatområden bör:

- veta vilka risker som faller inom deras ansvarsområden, den påverkan som dessa risker kan medföra för andra områden och de konsekvenser som kan följa av att andra områden påverkas av dessa risker
- ha nyckeltal eller indikatorer som gör det möjligt att följa upp viktiga verksamheter,

prestationer och resultat, nå uppsatta mål samt att upptäcka förändringar eller avvikelser som kräver åtgärder (t. ex. prognoser och budgetar)

- ha system som följer upp budgetar och prognoser med lämpliga mellanrum och rapporterar avvikelser så att åtgärder kan vidtas
- rapportera systematiskt och snabbt till högsta ledningen om man upptäcker avvikelser, nya risker eller att befintliga skyddsåtgärder inte fungerar

All personal bör:

- förstå sitt eget ansvar för att hantera enskilda risker
- förstå hur de kan medverka till ständig förbättring av riskhanteringen
- förstå att riskmedvetenhet och riskhantering är viktiga delar av organisationens kultur
- rapportera systematiskt och snabbt till ledningen om man upptäcker avvikelser, nya risker eller att befintliga skyddsåtgärder inte fungerar

7.2 Extern rapportering

En organisation behöver regelbundet avrapportera sin riskhantering till sina intressenter, däribland redogöra för sin policy för riskhantering samt vilka resultat och effekter som uppnåtts genom att följa denna. Intressenterna vill i allt högre grad få organisationer att redovisa hur väl man uppfyller sina egna och andras krav på icke-finansiella perspektiv, som att vara en god samhällsmedborgare, i form av sociala bokslut och miljöbokslut som t.ex. tar upp arbetsmiljö, hälsa och säkerhet eller arbete för mänskliga rättigheter.

God verksamhetsstyrning innebär att en organisation bedriver riskhantering med ett metodiskt angreppssätt för att:



- skydda intressenternas värden
- säkerställa att styrelsen utför sina uppgifter i fråga om att lägga fast strategin, skapa förädlingsvärden och följa upp organisationens prestationer
- säkerställa att ledningssystemet har erforderliga kontrollfunktioner och att dessa fungerar som de ska

Gången för den formella rapporteringen av riskhantering bör vara tydligt fastlagd och öppen för intressenterna att ta del av.

Den formella rapporteringen bör omfatta följande:

- kontrollfunktionerna - i synnerhet vad gäller ledningens ansvar för riskhantering
- de processer som används för att identifiera risker och hur de ingår i riskhanterings-systemet
- de primära kontrollsystem som finns i syfte att hantera betydande risker
- de uppföljnings- och granskningssystem som finns

Alla allvarliga brister och fel som systemet hittar, eller som finns i själva systemet, ska rapporteras tillsammans med de mått och steg som vidtagits för att åtgärda dem.

8. Riskhanteringsstruktur och administration

8.1 Riskhanteringspolicy

En organisations riskhanteringspolicy bör tydligt beskriva dess vilja och förmåga till risktagande och syn på vikten av riskhantering. Policyn bör också lägga fast ansvaret för riskhantering i hela organisationen.

Den bör också knyta an till gällande författningar och regelverk inom ramen för policyn, t.ex. arbetsmiljökrav och brandskydd

Till riskhanteringsprocessen hör också en samlad uppsättning metoder och tekniker för användning inom olika delar av verksamhetsprocesserna. För att fungera effektivt behöver riskhanteringsprocessen följande:

- stöd och engagemang från VD och verkställande ledningen
- fastläggande av ansvar inom organisationen
- erforderliga resurser för utbildning och förbättring av riskmedvetenheten i alla intressentled

8.2 Styrelsens roll

Styrelsen har ansvar för att fastställa organisationens strategiska inriktning och för att skapa förutsättningar så att risker kan hanteras effektivt.

Detta kan ske genom en ledningsgrupp, en samordningsgrupp, en revisionsgrupp eller någon annan funktion som passar organisationens sätt att arbeta, och som har möjlighet att fungera som huvudman för riskhantering.



Styrelsen bör som ett minimum beakta följande vid utvärdering av ett ledningssystem:

- *art och omfattning av de risker som en organisation finner acceptabla att ta i sin verksamhet*
- *sannolikheten för sådana exponeringar*
- *hur oacceptabla risker ska hanteras*
- *organisationens förmåga att minimera sannolikhet och påverkan på verksamheten*
- *risker och möjligheter med en aktivitet och vilka kontrollåtgärder som vidtagits*
- *riskhanteringsprocessens effektivitet*
- *hur styrelsen själv påverkar risktagandet*

8.3 Verksamhetsområdenas roll

Detta innefattar följande:

- *verksamhetsområdena har det primära ansvaret för att riskhantering är en del av den dagliga verksamheten*
- *ledningen för ett verksamhetsområde är ansvarig för att främja riskmedvetenheten i verksamheten*
- *verksamhetsmål för riskhantering bör införas*
- *riskhantering bör vara en stående punkt på dagordningen på ledningsgruppernas möten för att det ska ges tillfälle att ta hänsyn till riskexponeringar och att omprioritera i verksamheten på basis av löpande riskanalys*
- *ledningen för ett verksamhetsområde bör se till att riskhantering finns med redan i planeringsfasen av ett projekt och sedan fortlöpande genom hela projektet*

8.4 Riskhanteringsfunktionens roll

Beroende på organisationens storlek kan riskhanteringsfunktionen i fråga om personella resurser variera från en enda person på deltid eller heltid till en egen enhet.

Riskhanteringsfunktionen bör ha följande uppgifter:

- *att föreslå policy och strategi för riskhantering*
- *att vara huvudman för riskhantering på strategisk och operativ nivå*
- *att se till att bygga upp riskmedvetenhet som en del av organisationskulturen tillsammans med erforderlig utbildning*
- *upprätta en intern riskhanteringspolicy och struktur för verksamhetsområdena*
- *upprätta och granska processer för riskhantering*
- *samordna de olika funktioner som ger råd om riskhanteringsfrågor inom organisationen*
- *utveckla processer för att ta fram åtgärder mot risker inklusive beredskaps- och kontinuitetsplaner*
- *redovisa risker i rapporter till styrelse och övriga intressenter*

8.5 Internrevisionens roll

Rollen för internrevisionen kommer troligtvis att skilja sig åt mellan olika organisationer.

I praktiken kan den interna granskningen omfatta följande:

- *inrikta aktiviteterna på allvarliga risker som identifierats av ledningen och granska riskhanteringsprocesserna rakt igenom en organisation*



- *beskriva och intyga hur riskhantering bedrivs*
- *aktivt svara för stöd för och medverkan i riskhantering*
- *biträda vid riskidentifiering och riskvärdering samt utbilda personal om riskhantering*
- *samordna redovisning av risker och rapportering till styrelsen, internrevisionsgruppen etc.*

När man lägger fast en lämplig ordning i en organisation bör internrevisionen bevaka att man inte bryter mot de krav på oberoende och saklighet som gäller för internrevision.

8.6 Resurser och implementering

De resurser som krävs för att genomföra en organisations riskpolicy bör vara tydligt angivna på varje ledningsnivå och inom varje verksamhetsområde.

Utöver de befattningsbeskrivningar som kan finnas för ordinarie arbetsuppgifter bör de som arbetar med att samordna policy och strategi för riskhantering ha tydligt definierade roller. Samma tydliga definition krävs också för alla som arbetar med revision och granskning av ledning och styrning respektive biträder i riskhanteringsprocessen.

Riskhantering bör vara en del av strategi- och budgetprocesserna i varje organisation. Därigenom förankras också riskhantering i verksamheten genom den växelverkan som uppstår.

Riskhantering bör belysas vid introduktionskurser och all annan utbildning och kompetensutveckling liksom i verksamhetsprocesserna, t.ex. projekt för att utveckla produkter och tjänster.

9. Övervakning och granskning av riskhanteringsprocessen.

Effektiv riskhantering kräver en rapporterings- och granskningsstruktur för att säkerställa att risker identifieras och värderas enligt gällande policy och att lämpliga kontroller och skyddsåtgärder finns. Regelbunden revision av efterlevnaden av policy och riktlinjer ska utföras och riktlinjernas ändamålsenlighet ska granskas, så att man identifierar möjligheter till förbättring. Man ska komma ihåg att organisationer är dynamiska och arbetar i dynamiska miljöer. Ändringar i organisation och omvärld måste identifieras och lämpliga anpassningar av systemen måste göras.

Uppföljningsprocessen bör säkerställa att det finns lämpliga styrmedel för organisationens aktiviteter och att rutinerna har förståtts och att de följs.

Varje uppföljnings- och granskningsprocess bör avgöra om:

- *de införda åtgärderna resulterade i det som avsågs*
- *angreppssätt och underlag för värderingar varit lämpliga*
- *förbättrad kunskap skulle ha bidragit till bättre beslut*
- *lärdomar kan dras för framtida värdering och hantering av risker*



10. Bilaga

Riskidentifieringsmetodik- exempel

- *Tillbudsrapportering och uppföljning*
- *Revisioner och besiktningar*
- *HAZOP-analyser*

Risikanalysmetodik-exempel

Dynamiska risker

- *Marknadsundersökning*
- *Affärsplaner*
- *Provlansering*
- *FoU*
- *Känslighetsanalys*

Båda perspektiven

- *Flödes-och processschema/Beroenden*
- *SWOT-analys*
- *Händelsesträd*
- *Planering för ostörd verksamhet*
- *BPEST-analys*
- *Framtagande av alternativa möjligheter att bedriva verksamheten*
- *Beslutsfattande under risk*
- *Statistiska beslutsmodeller*
- *Medelvärde och variabilitet i beslutsunderlag*
- *PESTLE-analyser*

Statiska risker

- *Hotanalys*
- *Felträdsanalys*



AGERS - Asociación Española de Gerencia de Riesgos y Seguros
Príncipe de Vergara, 86 - 1ª Esc., 2º Izda.- 28006 Madrid - SPAIN
Tel: + 34 91 562 84 25 – Fax: + 34 91 590 07 80 – Email: gerencia@agers.es – www.agers.es



AIRMIC - The association of Insurance and Risk Managers
Lloyd's Avenue, 6 – London EC3N3AX - UK
Tel: + 44 207 480 76 10 – Fax: + 44 207 702 37 52 – Email: enquiries@airmic.co.uk – www.airmic.com



AMRAE - Association pour le Management des Risques et des Assurances de l'Entreprise
Avenue Franklin Roosevelt, 9-11 – 75008 Paris - FRANCE
Tel: + 33 1 42 89 33 16 – Fax: + 33 1 42 89 33 14 – Email: amrae@amrae.fr – www.amrae.fr



ANRA - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali
Via del Gonfalone 3, I-20123 Milano - ITALY
Tel: + 39 02 58 10 33 00 – Fax: + 39 02 58 10 32 33 – Email: anra@betam.it – www.anra.it



APOGERIS - Associação Portuguesa de Gestão de Riscos e Seguros
Avenida da Boavista, 1245, 3a Esq. – 4100-130 Porto – PORTUGAL
Tel: + 351 22 608 24 62 – Fax: + 351 22 608 24 73 – E-mail: anfernandes@sonae.pt – www.apogeris.pt



ASPAR CR - Association of Insurance and Risk Management of the Czech Republic o.s.
Nad Ohradou 7 – 13000 Praha 3 – Tel: + 420 602 384 256 – Email: asparcr@volny.cz



BELRIM - Belgian Risk Management Association
Rue Gatti de Gamond, 254 – 1180 Bruxelles - BELGIUM
Tel: + 32 2 389 23 95 – Fax: + 32 2 389 22 72 – Email: info@belrim.com – www.belrim.com



bfV - Bundesverband firmenverbundener Versicherungsvermittler und -Gesellschaften e.V.
c/o Mr Hans-Otto GEIGER – Postfach 1916 – D-67209 Frankenthal – GERMANY
Tel: + 49 6233 86 2507 - Fax: + 49 6233 86 2507 - Email: hans-otto.geiger@ksb.com – www.bfv-fvv.de



BRIMA - Bulgarian Risk Management Association
101, Tzarigradsko chaussee, floor 4 – Sofia 1113 – BULGARIA
Tel: + 359 878 100292 – Fax: + 359 2 971 0702 – Email: office@brima.biz – www.brima.biz



DARIM - DI's Risk Management Forening
DK-1787 Copenhagen – DENMARK
Tel: + 45 33 77 33 77 – Fax: + 45 33 77 33 00 – Email: darim@di.dk – www.di.dk



DVS - Deutscher Versicherungs-Schutzverband e.V.
Breite Strasse 98 - D 53111 Bonn - GERMANY
Tel: + 49 228 98 22 30 - Fax: + 49 228 63 16 51- Email: dvs@dvs-schutzverband.de – www.dvs-schutzverband.de



FINNRIMA - Finnish Risk Management Association
Talvikkitie 40 A 33, 01300 Vantaa – FINLAND
Tel: + 358 9 5607 5361 – Fax: + 358 9 5607 5365 – Email: srhy@hennax.fi – www.srhy.fi



NARIM - Nederlandse Associatie van Risk en Insurance Managers
P.O. Box 65707 - 2506 EA Den Haag – THE NETHERLANDS
Tel: + 31 70 345 7426 – Fax: + 31 70 427 3263 – Email: ielsdewild@imfo.nl – www.narim.com



POLRISK - Polish Risk Management Association
ul. Rzymowskiego 30 lok. 424 - 02-697 Warszawa - POLAND
Tel: + 48 22 331 8121 – Fax: + 48 22 331 81 22 – Email: info@polrisk.pl – www.polrisk.pl



RUSRISK - Russian Risk Management Society
Address Expert Institute, Staraya Ploshchad 10/4, Moscow, 103070 – RUSSIA
Tel: + 7 495 231 53 56 - Fax: + 7 495 231 53 56 - Email: info@rrms.ru – www.rrms.ru



SIRM - Swiss Association of Insurance and Risk Managers
Gutenbergstrasse 1, Postfach 5464, CH-3001 Bern - SWITZERLAND
Tel: + 41 31 388 87 89 – Fax: + 41 31 388 87 88 – Email: info@sirm.ch – www.sirm.ch

SWERMA - Swedish Risk Management Association
Gränsvägen 15 - SE-135 47 Tyresö - SWEDEN
Tel: + 468 742 13 07 - Fax: + 468 798 83 11- E-mail: info@swerma.se – www.swerma.se

ALARM - The National Forum for Risk Management in the Public Sector
Queens Drive, Exmouth - Devon, EX8 2AY
Tel: + 44 1395 223399 - Fax: + 44 1395 223304 - Email: admin@alarm.uk.com - www.alarm-uk.com



IRM - The Institute of Risk Management
6 Lloyd's Avenue - London EC3N 3AX
Tel: + 44 20 7709 9808 - Facsimile + 44 20 7709 0716 - Email: enquiries@theirm.org - www.theirm.org