BILAGA 1 FÖRORDNINGAR, BESTÄMMELSER, ANVISNINGAR

Förvaltningslag (434/2003)
Grunderna för god förvaltning, 610 §

Lag om statsbudgeten (423/1988), 24 b §
Ordnande av intern kontroll och ledningens ansvar

- Ämbetsverk och inrättningar ska se till att den interna kontrollen är ordnad på ett ändamålsenligt sätt i deras egen verksamhet samt i verksamhet för vilken ämbetsverket eller inrättningen svarar.
- Ämbetsverkens och inrättningarnas ledning skall leda ordnandet av den interna kontrollen och svara för att den är ändamålsenlig och tillräcklig.

Förordning om statsbudgeten (1243/1992)
Intern kontroll, innehåll och mål, 69 §

- Ämbetsverkens och inrättningarnas ledning skall se till att vid ämbetsverket eller inrättningen vidtas sådana med tanke på omfattningen av dess ekonomi och verksamhet och innehållet i dessa samt därtill anslutna risker ändamålsenliga förfaranden (intern kontroll).
- Genom dessa förfaranden säkerställs lagligheten i och resultatet av ekonomin och verksamheten, tryggandet av tillgångar och egendom och riktiga och tillräckliga uppgifter om ämbetsverkets eller inrättningens ekonomi och verksamhet som ledningen och den externa styrningen av ämbetsverket eller inrättningen förutsätter.
- Förfarandena skall också omfatta förvaltningen av de medel som ämbetsverket eller inrättningen skall svara för eller förmedla samt sådana funktioner och uppgifter som ankommer på ämbetsverket eller inrättningen men som har givits i uppdrag åt något annat ämbetsverk eller någon annan inrättning, en sammanslutning eller enskilda eller som ämbetsverket eller inrättningen annars svarar för.
- Servicecentralens ledning svarar för den interna kontrollen till den del som bokföringsenhetens uppgifter genom ett serviceavtal har överförts till servicecentralen.

Hänvisning till allmänna standarder och rekommendationer, 69 a §

- Vid förfarandena inom den interna kontrollen skall de verkningar som Europeiska gemenskapsrätten har med tanke på ämbetsverkets eller inrättningens verksamhet beaktas. Dessutom skall de allmänna standarder och rekommendationer som gäller intern kontroll beaktas.

Ekonomistadgans innehåll (69 b §)

- Av ekonomistadgan framgår noggrannare bestämmelser om intern kontroll och till den hörande faktorer som inverkar på hanteringen av risker.

Innehållet i verksamhetsberättelsen som ingår i bokföringsenhetens bokslut, 65 §

- Utlåtande om utvärdering och bekräftelse gällande den interna kontrollen

Innehållet i regeringens årsberättelse, 68 a § och 68 b §

- Riskbesiktningar i regeringens årsberättelse

Delegationen för intern kontroll och riskhantering, 71 §

Statskontorets föreskrift om utarbetande och uppdatering av ekonomistadgan (Dnr 481/03/2010, 23.11.2010)

- förfaranden vid intern kontroll genom vilka ledningen strävar efter att hålla de risker som ansluter till ekonomiförvaltningen på en kontrollerbar nivå

Statskontorets anvisning om upprättande av verksamhetsberättelsen (Dnr VK 510/03/2010, 30.11.2010)

- utlåtande om utvärdering och bekräftelse gällande den interna kontrollen

Statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010)

- de allmänna kraven på informationssäkerhet i fråga om handläggning av dokument
- tillgodoseende av informationssäkerheten inklusive de informationssäkerhetsrisker som hänför sig till myndighetens verksamhet kartläggs, 5 §

Arbetarskyddslag (738/2002)

- arbetsgivarens allmänna omsorgsplikt, 8 §
- utredning och bedömning av riskerna i arbetet, 10 §

Övriga förordningar, bestämmelser, riktlinjer och handlingar som ansluter till [ämbetsverkets] riskhantering

[Här nämns eventuella övriga till riskhantering anslutna nationella författningar eller EU:s rättsakter, bestämmelser baserade på internationella avtal, arbetsordningen, ekonomistadgan, principer för riskhantering som ansluter till förvaltningen av statens förmögenhet och ansvarsområden (VAHTI:s anvisningar), arbetarskyddets handböcker om riskhantering, särskilda handlingar om riskhantering enligt bransch o.dyl.]

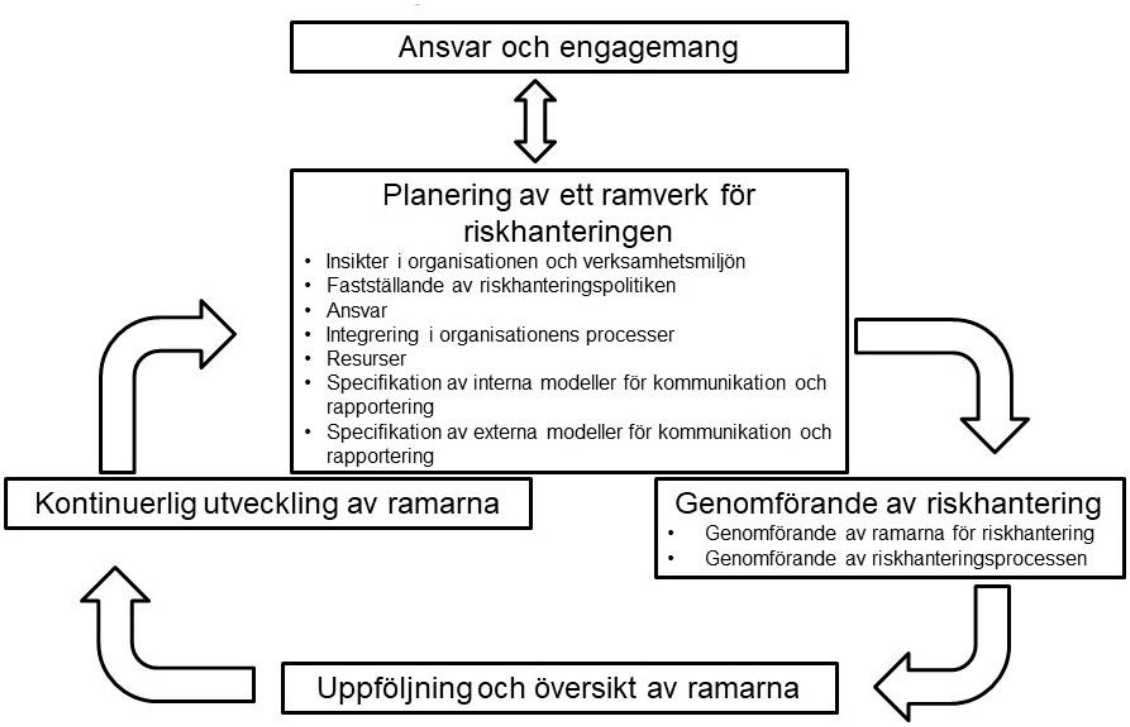
BILAGA 2 BEGREPPSDEFINITIONER

[Av förteckningen nedan framgår de viktigaste begreppen inom riskhantering inklusive definitioner. [Ämbetsverken kan själva välja vilka som är de viktigaste och komplettera listan vid behov.]

Kvarstående risk	En risk som återstår efter att en risk behandlats och som det inte går att undanröja eller som man inte vill undanröja. Kvarstående risker kan innebära oidentifierade risker.
Risk	Osäkerhetens effekt på målen. Effekten utgör en avvikelse från det förväntade. Effekten kan vara positiv eller negativ i jämförelse med den förväntade effekten.
Riskanalys	En process med vars hjälp man försöker förstå riskens karaktär och fastställa risknivån. En riskanalys utgör grunden för uppskattningen av riskens betydelse och för beslut som gäller riskhantering. Riskanalysen innebär en bedömning av riskens storlek.
Riskbedömning	En genomgripande process som innefattar den riskidentifierande riskanalysen och uppskattningen av riskens betydelse.
Riskhantering	En bearbetningsprocess gällande risken där man bestämmer om t.ex. följande åtgärder: – avvärja eller undanröja risken genom beslut om att låta bli att inleda eller fortsätta verksamhet som förorsakar en risk – ta en risk eller öka risken för att nå en möjlighet – undanröja riskkällan eller riskorsaken – ändra eller inverka på sannolikheten – ändra eller bereda sig på konsekvenserna – dela risken med en annan eller andra parter – kvarhålla och utstå risken genom ett kunskapsbaserat beslut
Identifiering av risker	Process för observation och beskrivning av riskerna
Riskhantering	Samordnad verksamhet som leder och styr organisationer i fråga om risker.
Riskhanteringspolitik	Principer och mål relaterade till riskhantering som organisationen beslutat om och dokumenterat.
Riskhanteringsprocess	Systematisk tillämpning av principer, förfaranden och praxis gällande fastställandet av verksamhetsmiljön, identifiering, analysering, uppskattning, hantering och uppföljning av risker samt kommunikation och informationsutbyte.
Riskhanteringsplan	En av ledningen godkänd och dokumenterad handlingsplan för riskhantering
Riskkriterier	Regler enligt vilka riskens betydelse bedöms på ett enhetligt sätt. Riskkriterierna baserar sig på organisationens mål och verksamhetsmiljö. Riskkriterierna kan ha härletts ur standarder, lagar, verksamhetsprinciper och andra krav.
Riskklassifikation	Hjälpmedel för klassifikation av objekt som ska utvärderas.
Riskmatris	Med hjälp av riskmatrisen klassificeras riskens storlek utifrån hur allvarliga konsekvenserna av händelsen är och utifrån sannolikheten för att en risk föreligger. Matrisen underlättar gestaltning av riskens betydelse och hur risken förhåller sig till andra risker.
Metod för riskhantering	Åtgärd som förändrar risken Hanteringsmetoder är alla processer som ändrar på risken, verksamhetsprinciper, instrument, praxis eller andra åtgärder. Hanteringsmetoderna har nödvändigtvis inte alltid önskad eller uppskattad ändringseffekt.

Uppskattning av riskens betydelse	En process där man genom att jämföra riskanalysens resultat med riskkriterier bestämmer om risken eller riskens omfattning är godtagbar eller dräglig. Uppskattningen av riskens betydelse underlättar beslut om hantering av risken.
Riskens ägare	Person eller aktör som har ansvar och behörighet att hantera risker. Ofta utses även en ansvarig person för riskåtgärder. Denna person följer i praktiken upp och samordnar en viss risk.
Risknivå	Riskens omfattning eller omfattningen av kombinationerna av risker som anges som en kombination av följderna och följdernas sannolikhet (t.ex. utkomsten av konsekvensen och sannolikheten)
Intern revision	Den interna revisionen har i uppgift att för ledningen redogöra att den interna kontrollen är ändamålsenlig och tillräcklig.
Intern kontroll	Förfaranden som säkerställer – lagligheten i och resultatet av ekonomin och verksamheten, – tryggandet av tillgångar och egendom, – riktiga och tillräckliga uppgifterna om ämbetsverkens och inrättningarnas ekonomi och verksamhet

BILAGA 3 RAMAR FÖR RISKHANTERING



källa: Med tillstånd av SFS-ISO 31000, SFS

BILAGA 4 RISKHANTERINGSPROCESSEN

Nedan beskrivs *[ämbetsverkets]* riskhanteringsprocess. *[Ämbetsverket ska utforma processen så att den passar ämbetsverkets egen riskhantering och skriva nödvändiga organisationsspecifika anvisningar.]*

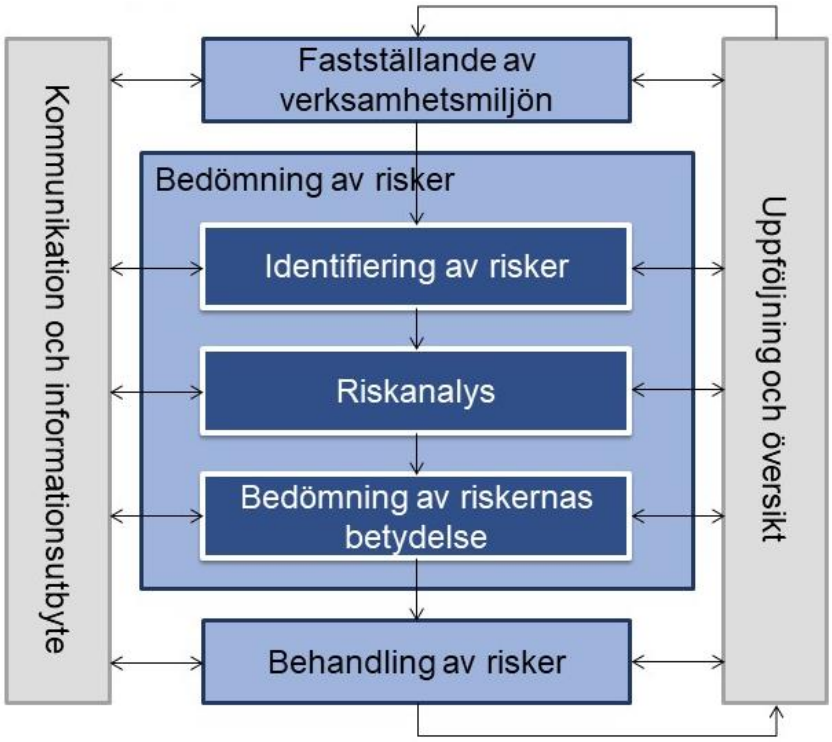


Bild Riskhanteringsprocessen, med tillstånd av Finlands Standardiseringsförbund SFS, SFS ISO 31000

1 Fastställande av verksamhetsmiljön

I det skede av riskhanteringsprocessen när verksamhetsmiljön fastställs, görs de viktigaste avgränsningarna gällande uppskattningen av risker, dvs. vad inberäknas i uppskattningen och vad lämnas utanför. I det här skedet fastställs även riskkriterierna som utnyttjas i ett senare skede när riskernas betydelse uppskattas och hanteringsmetoden väljs. I samband med dessa beaktas bl.a. strategier, mål, verksamhetsmiljön, intressenter, författningar och andra krav. Riskkriterierna fastställer även på vilken nivå riskerna är godtagbara eller drägliga.

2 Riskbedömning

Till riskbedömning hör identifiering av risker, riskanalys, dvs. analys av sannolikheten för och konsekvenserna av risker samt en uppskattning av riskernas betydelse.

2.1 Identifiering av risker

Målet i samband med identifieringsskedet av risker är att observera alla signifikanta risker och källorna till dessa, omfattning, händelser och orsakerna därtill samt eventuella följder. Här sammanställs information om risker som äventyrar verksamheten och möjligheten att nå målen

samt om de risker inbegriper möjligheter som man inte tidigare identifierat. För att identifiera risker behövs tillräckligt med sakkunniga för att säkerställa en övergripande lägesbild.

I samband med att riskerna identifieras framställs en förteckning över de risker vars sannolikhet och konsekvenser uppskattas i det skede riskerna analyseras. För att klassificera risker används olika kategorier (bilaga5): 1. Strategiska risker, 2. Operativa risker, 3. Ekonomiska risker, 4. Skaderisker.

2.2 Riskanalys

Riskanalysens syfte är att bilda en uppfattning om identifierade risker. I detta skede granskas orsakerna och källorna till riskerna, positiva och skadliga konsekvenser av riskerna. Därutöver uppskattas sannolikheten för att risken blir verklig och konsekvensen av detta på en förutbestämd skala (bilaga 6):

Sannolikhet: 1. Osannolik, 2. Potentiell, 3. Sannolik, 4. Högst sannolik.

Verkning: 1. Ringa, 2. Måttlig, 3. Betydande 4. Kritisk.

Som ett resultat av riskanalysen fås

- en enhetlig bild av sannolikheten för risker från fall till fall och verkningarna av dessa
- en bild av faktorer och beroendeförhållanden som inverkar på att risken blir verklig, orsaker till att risken blir verklig.
- en grund för bedömningen av vilken betydelse risken har, dvs. en grund för vilka åtgärder som vidtas och vilka man låter bli att vidta i fråga om riskerna

2.3 Uppskattning av riskernas betydelse

Målet för uppskattningen av riskernas betydelse är att underlätta beslutsfattandet. Vilka risker ska hanteras och i vilken ordning. Prioritetsordningen utgår ifrån sannolikheten och verkningarna. Riskmatrisen (bilaga 7) gör det enklare att få en uppfattning om riskernas betydelse och göra en bedömning av den. Är risken godtagbar eller behöver ärendet hanteras.

Även om en risk inte är av betydelse, kan den i kombination med en annan risk få betydelse. I samband med uppskattningen bör eventuella redan bestämda/planerade åtgärder beaktas. Är de tillräckliga eller är den kvarstående risken sådan att eventuellt andra åtgärder behövs för att man ska kunna hantera risken.

Genom att uppskatta riskernas betydelse får man

- en organiserad förteckning över risker
- en enhetlig bild av risker som ska behandlas för att man ska kunna planera åtgärder.

3 Riskhantering

I samband med riskhantering bestäms vilka fortsatta åtgärder som vidtas och vilka ansvariga personer som utses samt en preliminär tidtabell görs upp. I detta skede bestämmer man även om de kvarstående riskerna är drägliga. Alternativ för riskhantering:

- avvärja en risk t.ex. genom att avstå från den verksamhet som leder till en risk
- ta eller öka en risk för att uppnå en möjlighet
- undanröja riskkällan eller riskorsaken
- ändra sannolikheten för en risk
- ändra verkningarna av en risk
- dela risken med andra parter

- kvarhålla en risk utifrån ett kunskapsbaserat beslut

Av dess alternativ kan en eller flera riktas på en risk

Åtgärderna, sannolikheten för dessa, ansvaren och tidtabellerna dokumenteras i **riskhanteringsplanen**. Åtgärderna ska anpassas i förhållande till hur stor risken är och de ska vidtas på den organisationsnivå som är avsedd för ändamålet. Även kvarstående risker dokumenteras så att de kan följas upp och vid behov behandlas på nytt. Riskhanteringsplanen godkänns av ämbetsverkets högsta ledning. De mest påfallande riskerna och till dessa relaterade hanteringsåtgärder ska antecknas i för ändamålet lämpliga planer och uppföljningen av åtgärderna i uppföljningsrapporter.

Resultatet av riskhanteringen ger
- en helhetsbild av riskerna, risknivån, hanteringsåtgärderna, ansvaret och tidtabellen

4 Uppföljning

Uppföljning och granskning utgör viktiga moment gällande slutförandet av riskhanteringsprocessen och säkerställer verkningarna och effekten av valda åtgärder. Det ger även information om hur riskhanteringen i organisationen lyckas. Det här skedet innefattar iakttagelse av interna och externa förändringar av verksamhetsmiljön och förändringar av risker samt eventuella av att ändra riskkriterierna. Åtgärderna som gäller uppföljning och granskning kan vidtas med jämna intervaller eller i vissa lägen. Ansvar som gäller dessa ska anges.

I detta skeda är det möjligt att intervenera om riskerna håller på att bli obehandlade.

5 Kommunikation och informationsutbyte

Riskbedömningen förutsätter kommunikation mellan olika parter som berörs av verksamhetsmiljön och riskerna. Tack vare kommunikationen når uppgifterna om riskerna dem som ska känna till dessa och den information som är nödvändig för riskhantering kan fördelas mellan dem som är ansvariga för åtgärderna och kontrollen. Kommunikationen inom riskhanteringen ska upptas i riskhanteringsplanen.

I kommunikationen gällande riskhantering ingår alla väsentliga risker och åtgärder. Till detta hör även ett betryggande informationsutbyte mellan ämbetsverkets, samarbetspartner och intressenter. Uppgifter om ämbetsverkets påtagliga risker och riskhanteringsåtgärder rapporteras till den som svarar för resultatstyrningen.

BILAGA 5 RISKKLASSIFIKATION

Riskklassifikationen gör det lättare att få en helhetsbild av riskerna. Nedan presenteras en allmän klassifikation som man rekommenderar att används i samband med riskbedömning. *[Vid behov kan ämbetsverket specificera en noggrannare klassifikation eller använda en annan indelning som bättre tjänar ämbetsverkets riskhantering.]*

1. Strategiska risker
t.ex. strategi, verksamhetsmiljö, konjunkturförändringar, författningsändringar, ledningssystemet, organisationsstrukturen, värderingar, etiska principer, kommunikation, image, intressenter, samarbetspartner

2. Operativa risker
t.ex. verksamhetens mål, planering och organisering av verksamheten, verkställande av beslut, personal, processer, anskaffningar, avtal, kvalitet, kunder, branscher, arbetsredskap, teknologi, informationsförvaltning, informationssystem, datasäkerhet, cybersäkerhet

3 Ekonomiska risker
t.ex. finansiering, budgetering, ekonomiplanering, användning av tillgångar, förmögenhet, ekonomiskt ansvar, statlig garanti och borgen, ekonomirapporter

4. Skaderisker
t.ex. säkerhet i verksamhetslokal, maskiner, instrument, arbetarskydd, arbetshälsa, olyckor, personsäkerhet, resor, miljöförstöring

BILAGA 6 RISKANALYS: SANNOLIKHET OCH KONSEKVENS

Nedan presenteras en skala för bedömning av sannolik *[Vid behov kan ämbetsverket specificera eller använda en annan skala som bättre tjänar ämbetsverkets riskhantering.]*

Riskens sannolikhet

1. Osannolik: Händelsen blir verklig bara under avvikande förhållanden. Potentiell närmast i teorin, ingen kännedom om att det skulle ha hänt.

2. Potentiell: Händelsen kan ske i vissa fall. Händelsen har ägt rum ibland hos oss, ibland annanstans.

3. Sannolik: Händelsen sker eller har skett ofta eller flera tillbud har förekommit.

4. Högst sannolik: Händelsen förväntas ske med största sannolikhet.

Riskens verkning

1. Ringa: Om risken blir sann är verkningarna ringa med tanke på uppfyllandet av de strategiska målen.

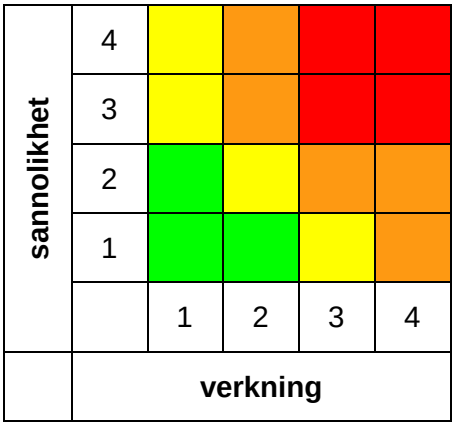
2. Måttlig: Om risken sker fördröjer och försvagar det tydligt möjligheterna att nå det strategiska målet. Verkning eller händelse utifrån vilken det inte är nödvändigt att avbryta verksamheten, men åtgärdsrelaterade planer är eventuellt nödvändigt att ändra. Ringa kostnader kan uppstå till följd av händelsen. Anseendet som en pålitlig aktör äventyras.

3. Betydande: Om risken sker, försvårar, fördröjer eller för övrigt äventyrar det på ett avsevärt sätt att ett viktigt strategiskt mål uppfylls. Om risken sker kan det leda till avsevärda skador och kostnader. En följd eller händelse på grund av vilken verksamheten måste avbrytas eller som en följd av händelsen uppstår lite större kostnader. Händelsen kan även leda till att egendom går sönder. Den enskilda människans hälsa kan äventyras. Anseendet som en pålitlig aktör försvagas.

4. Kritisk: Om risken sker, förhindrar eller avbryter det helt ur verksamhetens synvinkel att ett viktigt strategiskt mål uppfylls. Av att risken blir verklig kan stora skador och kostnader även för andra följa. En följd eller händelse på grund av vilken verksamheten måste avbrytas och verksamheten förhindras för en längre tid. Händelsen kan leda till avsevärda kostnader sett ur hela statsförvaltningens synvinkel. Hälsan hos en stor grupp människor och människoliv äventyras och det kan ha en omfattande verkan på hela samhällets funktion. Finlands anseende eller ställning i internationella sammanhang äventyras.

BILAGA 7 RISKMATRIS

Risknivåerna kan beskrivas med hjälp av matriser i vilka riskerna placeras utifrån sannolikheten och verkningarna. Färgerna underlättar beskrivningen av riskernas betydelse och nödvändiga åtgärder.



Ur risknivån kan behovet av hantering härledas

Nivå	Behov av hantering
Kritisk risk (risktal 9-16)	• kräver i allmänhet omedelbara åtgärder • förutsätter kontinuerlig uppföljning
Betydande risk (risktal 4-8)	• uppgiften är en plan att minska risken • uppföljas
Måttlig risk (risktal 3-4)	• åtgärder behövs nödvändigtvis inte • följa upp risken och eventuell utveckling av den
Låg risk (risktal 1-2)	• kräver inga akuta åtgärder

Det finns fler matriser t.ex. i VAHTIs riskhanteringsanvisning.

BILAGA 8 RISKHANTERINGSPLAN

Exempeltabell som stöd för riskhanteringsprocessen och för riskhanteringsplanen

Namnet på risken	Beskrivning av risken	Risk-klass	Sannolik-het	Verkning	Risk-nivå	Behovet av hantering	Beskrivning av åtgärden	Kostnader och andra verkningar till följd av åtgärden	Ansvarig person	Tidtabell	Status

Ytterligare material finns i VAHTIs riskhanteringsanvisning.

REFERENSMATERIAL FÖR RISKHANTERING

Riskikompassi www.riskikompassi.fi

SFS-ISO 31000-standard ”Riskhantering. Principer och anvisningar”

SFS, Teknisk rapport, ISO/TR 31004:fi ”Riskienhallinta. Ohjeita standardin ISO 31000 soveltamisesta.

COSO ERM-referensram: Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Managemet – Integrated Framework

INTOSAIs kodex för god förvaltning: International Organization of Supreme Audit Institutions, INTOSAI GOV 9130

VAHTIs anvisningar

Anvisning för riskhantering, Finansministeriets publikationer 22/2017, http://urn.fi/URN:ISBN:978-952-251-862-0

Riskhanteringsinstrument - Excel - originalversion

Riskhanteringsinstrument - Excel - mer omfattande version

Anvisning för riskhantering instrumentet