Exempel på stiftelsers riskhantering

SÄÄTIÖT JA RAHASTOT

STIFTELSER OCH FONDER

Stiftelser och fonder rf, Helsingfors 2022

Författare: VD Liisa Suvikumpu, Stiftelser och fonder rf.

Styrgrupp:
Ordf., föreningsmedlem Paula Salovaara, Föreningen Konstsamfundet
Styrelseordförande Petteri Karttunen, Saastamoisen säätiö
Verksamhetsledare Elli Dahl, Yrjö Jahnssonin säätiö
Ombud Arto Mäenmaa, Jenny ja Antti Wihurin rahasto

Grafisk layout och infografik:
Anne Kaikkonen, www.timangi.fi

Översättning:
Heidi Granqvist

ISBN 978-952-68460-7-1 (pdf)

Stiftelser och fonder rf är en förening för finländska stipendiegivare, den enda intresse- och understödsföreningen för stiftelser i Finland. Våra drygt 200 medlemmar stöder årligen vetenskap, konst och annan samhällelig utveckling med totalt över en halv miljard euro.
Våra medlemmar följer **God stiftelsepraxis**. www.saatiotrahastot.fi/sv/

Innehåll

> God förvaltning är den bästa garantin för stiftelsens riskhantering.

Varför har vi skrivit denna handbok?

Risker hör livet till och ingår även i stiftelsernas verksamhet. Det är omöjligt att undvika alla risker hur väl man än förbereder sig, och å andra sidan tas risker också medvetet, exempelvis i placeringsverksamheten. God riskhantering ger stiftelserna möjlighet att uppnå sina syften samt att upprätthålla och utveckla sin verksamhet.

Denna handbok uppmuntrar stiftelser att bedöma sina risker och göra upp en plan för riskhanteringen. En välfungerande stiftelse gör upp en egen riskhanteringsplan eller kartläggning av compliance, som även uppdateras och följs upp regelbundet. Handbokens syfte är att samla grundläggande information om ämnet som är relevant för stiftelser samt presentera några exempel på hur riskhantering kan genomföras i praktiken.

Tanken med exemplen är att ge information om hur kolleger har gjort och underlätta för stiftelser att ta fram egna riskhanteringsplaner. Stiftelserna är olika och därför är det omöjligt att ta fram en enda modell för riskhantering som skulle passa alla, men vissa grundelement ingår alltid. Varje stiftelse anpassar sina processer och anvisningar utgående från sin specifika verksamhet.

Compliance-programmets delområden (Ratsula 2016).

Vad är riskhantering och varför är det viktigt också i stiftelser?

Riskhantering, kontinuitetsplanering, compliance. Detta är något som omfattar många olika sidor och delområden. Termen compliance används ofta också i Finland i fråga om riskhantering. Den syftar traditionellt på regelefterlevnad, alltså att verksamheten följer etablerade regler, direktiv och lagar eller på processen för att uppnå det.

Riskhantering ingår i stiftelsens prognostisering, strategiska planering och operativa verksamhet. Förlust av en medarbetare, avbrott i datatrafiken eller eldsvåda är praktiska exempel på olyckor som kan inträffa när som helst. Riskerna kan också vara osynliga hot, som en global finanskrasch, pandemi eller att stiftelsen inte uppnår sina mål.

Vanligtvis har stiftelsen en viss uppfattning om sina risker, men bara sällan en skriftlig plan för att undvika dem. Det är även svårt att mäta nyttan av riskhantering, så därför är en medveten ledning av compliance-verksamheten i stiftelserna fortfarande ovanlig. Å andra sidan har stipendiestiftelserna med konkret självreglering lyckats etablera compliance-verksamhet utan att den uttryckligen skulle ha kallats riskhantering eller compliance.

Riskhanteringen inom stiftelser ska helst göras systematiskt och kontinuerligt, eftersom omvärlden förändras hela tiden. Samhället har även förväntningar på allmännyttiga stiftelser på grund av deras särskilda ställning. Därför är utöver lagenlighet också god förvaltningspraxis, öppenhet, anseendehantering och starka processer för intern kontroll viktiga delar av stiftelsernas riskhantering.

Minimikravet på stiftelsens riskhantering är att uppfylla alla lagstadgade skyldigheter – och för Stiftelser och fonder rf:s medlemmar att följa *God stiftelsepraxis*.

OMSORGSFULL VERKSAMHET I STIFTELSEN

Enligt Maijala (2021).

Hur komma igång med hantering av riskerna?

Tillräcklig dokumentering

Vissa stiftelser har en handbok eller instruktioner för sin verksamhet. Många har sammanställt olika listor över sina kärnfunktioner och ansvarsfördelningen. Det finns stiftelser som skriver så ingående föredragningslistor och protokoll för styrelsen att det utifrån dem går att kontrollera ärendenas förlopp. Sådana dokument ger ändå inte tillräcklig och snabb hjälp när en allvarlig och överraskande incident inträffar.

Vilka dokument vore det viktigt för stiftelsen att åtminstone ha? I handboken *God förvaltning i stiftelser* listas följande som rekommenderade anvisningar för stiftelser:

ANVISNINGAR GER STÖD

Anvisningar och principer som styr förvaltningen

- förvaltningsrådets arbetsordning
- utnämningsutskottets arbetsordning
- principer för medelsförvaltning (innehåller anvisningar för placeringspolitiken och egendomsförvaltningen)
- ekonomireglemente
- principer för riskhantering och övervakning
- arvodes- och närståendekretsanvisning
- personalreglemente
- koncernstrategi

Introduktion och ”fyra ögon”

En bra dokumentation av stiftelsens verksamhet och praxis hjälper såväl nya förtroendevalda som tillfälligt eller kortvarigt anställda. Men utöver att läsa manualer och anvisningar ska nyanställda också få personlig introduktion. Det är bra att ha en separat plan för introduktionen, med inskrivna tidsmässiga mål och ansvarig(a) från den operativa ledningen och styrelsen.

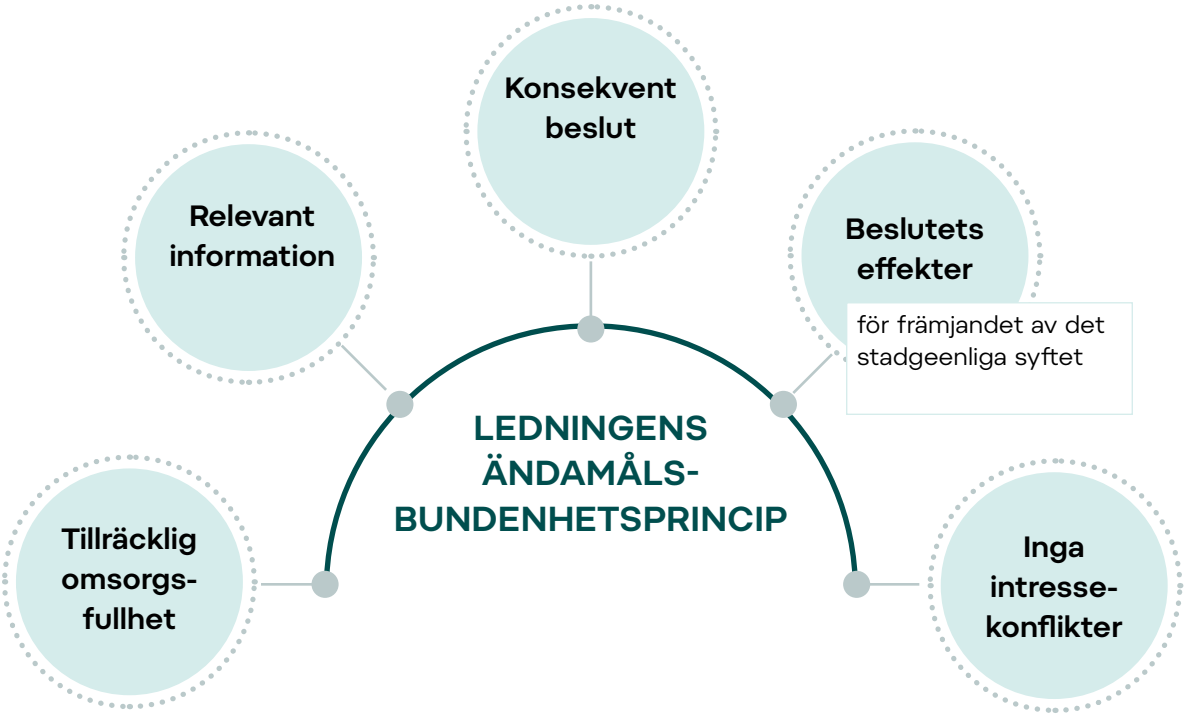
I god riskhantering ingår också grundprincipen för god förvaltning att undvika farliga arbetskombinationer. Konkret innebär det att inga funktioner slutförs utan att minst två olika personer har bedömt eller gått igenom dem. Det viktigaste är att en och samma person inte handhar hela processen från början till slut, utan exempelvis den som godkänner en faktura eller ett stipendium i systemet är en annan än den som genomför betalningen. Två par ögon ser mer än bara ett.

Anvisningar och principer som styr den operativa verksamheten

- strategi och verksamhetsplan
- budget
- ombudets/verkställande direktörens befattningsbeskrivning och befogenheter
- stipendiereglemente
- kommunikationsprinciper
- dataskyddsanvisningar
- arbetarskyddets åtgärdsprogram
- företagshälsovårdens verksamhetsplan
- verksamhetsanvisningar och principer som gäller annan operativ verksamhet

Ledningens krav på omsorgsfullhet och ansvarsförsäkringar

Enligt stiftelselagen (1:4) ska stiftelsens ledning omsorgsfullt främja fullgörandet av stiftelsens ändamål och stiftelsens intressen. Stiftelsens ledning – styrelsemedlemmarna och den operativa ledningen – har en uppdaterad, korrekt och heltäckande uppfattning om riskerna som gäller stiftelsen samt riskhanteringens ansvarsfördelning och uppföljning. Riskbedömning utgör en viktig del av årsplaneringen för att säkerställa kontinuiteten i stiftelsens verksamhet.



Stiftelserna är ofta små organisationer och därför sårbara. Stiftelsens styrelse bär ett stort ansvar. Styrelsen ansvarar för tillsynen av stiftelsen och dess ledning, så styrelsen måste definiera målen och metoderna för stiftelsens riskhantering samt intern rapporteringspraxis.

Styrelsen måste även fortlöpande bedöma hur väl samarbetet mellan styrelsen och den operativa ledningen fungerar. Ur riskhanteringssynvinkel handlar ledningsrisken om huruvida styrelsen är nöjd med VD:s verksamhet och att stiftelsen operativt leds på ett så bra sätt som möjligt.

Medlemmar i ledningen kan bli ersättningsskyldiga för beslut de fattat och ärenden de skött eller för att ha försummat dem. Medlemmar i förvaltningsorganen ansvarar i regel solidariskt för skador orsakade av beslut de fattat. Styrelsen befrias inte från sitt skadestånds- eller straffansvar, även om förvaltningsrådet skulle bevilja styrelsemedlemmarna ansvarsfrihet. Med tanke på ansvar och påföljder spelar det ingen roll om ett dåligt beslut har fattats av oaktsamhet eller på grund av ett bristande tillvägagångssätt. Det lönar sig för stiftelsen att teckna en ansvarsförsäkring för förvaltningen som täcker ekonomiska skador orsakade samfundet eller en utomstående, för vilka den försäkrade har skadeståndsansvar i egenskap av medlem i ett förvaltningsorgan.

Enligt en färsk utredning (EY Global Board Risk Survey 2021) har styrelser med föredömlig riskhantering tre nyckelfaktorer gemensamt:

- långsiktigt perspektiv på riskerna
- riskhanteringens prioriteringar fastställda enligt strategin
- fokus på stigande, otypiska och externa risker.

> Omfattningen av stiftelsens verksamhet och storleken på stiftelsetillgångarna som stiftelsen förvaltar framhäver styrelsemedlemmarnas skyldighet till aktiv verksamhet. HD 2020:93

Planering av riskhantering i praktiken: process och genomförande

Identifiering och bedömning av risker

Stiftelsen måste allra först förstå vilka risker som kan förknippas med den egna verksamheten. Mängden av alla risker man kan tänka sig i en stipendiestiftelse är stor, men alla risker kräver inte åtgärder. Det centrala är att fundera över vilka risker som är av betydelse för den egna stiftelsen och varför – vilken risk vill man att absolut inte ska förverkligas.

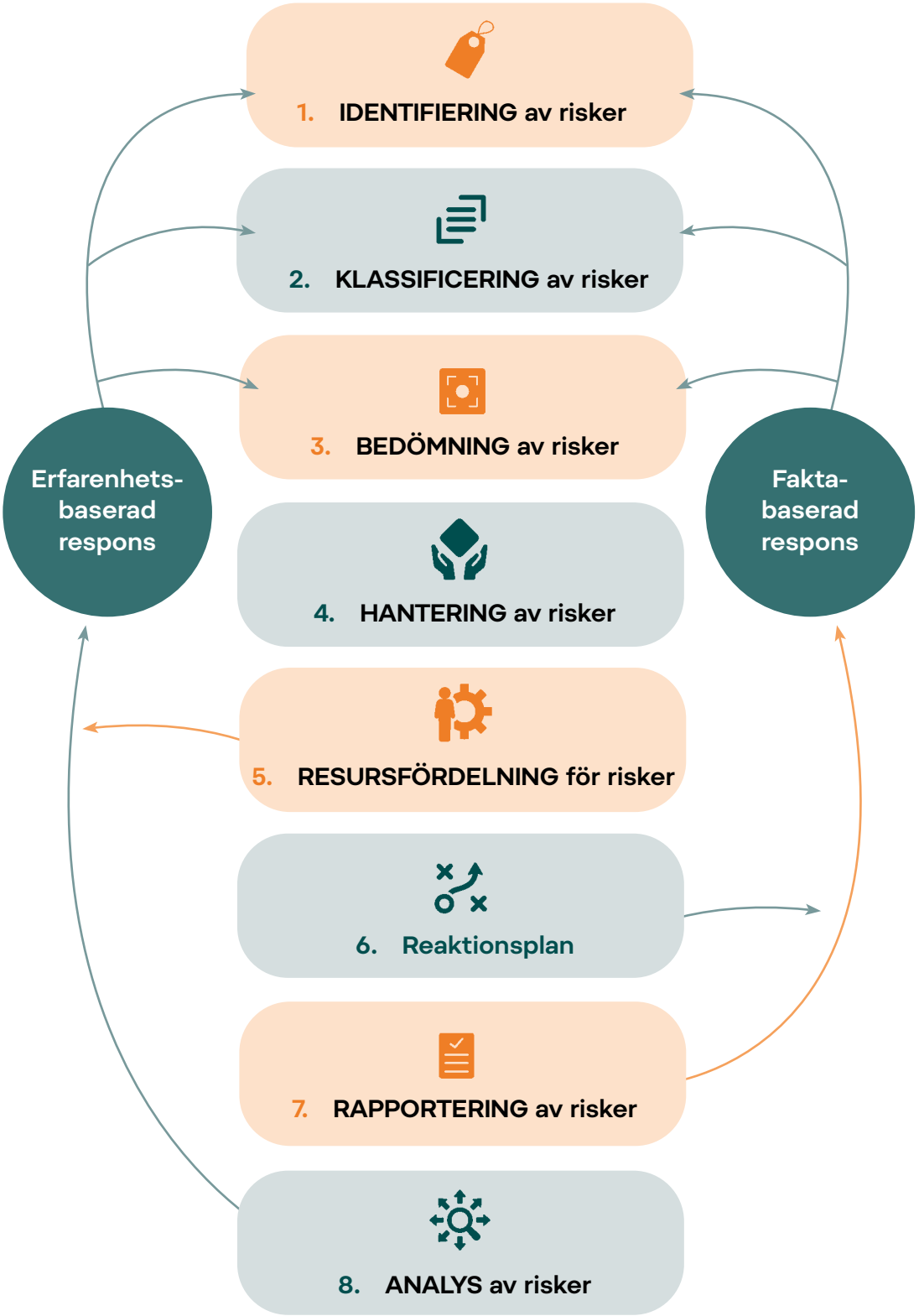
Bedömning och hantering av risker är en fortlöpande process. För att stiftelsens verksamhet ska vila på en stabil grund och vara kontinuerlig, är det en bra idé för styrelsen att införa riskhantering som en del av årsklockan.

Riskhantering är även hela personalens uppgift, eftersom alla som arbetar vid stiftelsen ska vara uppmärksamma på avvikelser från den normala verksamheten och rapportera dem vidare till sin chef eller stiftelsens ledning.

Varje stiftelse måste välja nivå för sin riskhantering och risktålighet, som även kan variera enligt situation och funktion. Resursfördelningen är avgörande för hur väl risker kan observeras och hur man hinner och kan reagera på dem: ju bättre överblick, desto större kostnader för riskhantering.

Riskhanteringens steg förenklat:

1. bedömning av vilka risker som kan förekomma
2. analys av riskerna och notering av vilka följder realiserade risker skulle ha och hur sannolikt det är att de förverkligas
3. beslut om riskhanteringssätt, ansvarsfördelning, åtgärder och allokering av tillräckliga resurser.



Riskhanteringsprocessen (Hopkin 2017).

Plan för riskhantering/kontinuitet

En plan för riskhantering och/eller kontinuitet tas fram för den eventualitet att stiftelsens verksamhet skulle hotas av en störning. Existensen av en riskhanteringsplan betyder att man redan i förväg har funderat över lösningar på problem som eventuellt kan dyka upp. I dokumentet har stiftelsen antecknat processen för att förebygga risker samt de preliminära idéerna för åtgärder ifall problemen realiseras.

Syftet med en skriftlig plan är att säkerställa att stiftelsen även i överraskande situationer ska kunna fortsätta sin verksamhet så väl som möjligt, att dess kritiska funktioner inte äventyras exempelvis om en nyckelperson plötsligt blir sjuk och att den dagliga förvaltningen inte avbryts.

Stiftelsen gör upp planen enligt sina egna behov och deras omfattning. Planen kan bestå av olika delar och utformas på olika sätt, men det viktiga är att den är tydlig och informativ.

Riskhanterings- och/eller kontinuitetsplanen är ett skriftligt dokument skapat utifrån bedömningsarbetet och innehåller åtminstone

- en lista över eventuella risker, deras sannolikhet, följdernas allvarlighetsgrad samt förslag till åtgärder
- samlade anvisningar och uppgifter som är tillgängliga för hela stiftelsen vid behov
- utsedda kontakt- och ansvarspersoner för varje punkt
- olika program, apparatur och olika tjänsteleverantörers kontaktinformation
- en bedömning av hur länge stiftelsen klarar ett avbrott, kontinuitetshanteringens åtgärder samt hur kommunikationen om läget sker

Planen kan innehålla en tabell med riskerna som är mest relevanta ur stiftelsens synvinkel, med den bedömda sannolikheten för att de ska inträffa, följdernas allvarlighetsgrad samt åtgärder och ansvarsfördelning för riskhantering. Det är enklast att skapa en överblick om riskernas sannolikhet och allvarlighetsgrad uttrycks med så kallade trafikljus.

Vilka risker kan stiftelser utsättas för?

RISKTYPER

Risker kan indelas i olika kategorier – även om gränserna mellan olika risktyper är flytande och de delvis är överlappande. I sin riskartläggning är det bäst att stiftelsen bedömer sin verksamhet i relation till alla risktyper, eftersom en fördjupning i dem kan bidra till att identifiera eventuella hot och störningar som är relevanta för den egna stiftelsen. Ibland kan en viss incident vara kopplad till en annan, så att en risk som betraktats som obefintlig eller liten plötsligt realiseras och påverkar många olika delområden av stiftelsens verksamhet.

Strategiska risker

De största av stiftelsens strategiska risker är sådana som äventyrar genomförandet av stiftelsens syfte. Strategiska risker är alltså inte enbart aspekter som sammanhänger med stiftelsens aktuella strategi, utan många olika risker kan vara strategiskt betydande.

Samhälleliga och politiska risker

Samhället i Finland är stabilt och därför förekommer det bara sällan att samhälleliga eller politiska risker realiseras snabbt i stiftelsernas omvärld. Den bästa långsiktiga riskhanteringen för stiftelser är att följa och aktivt delta i den egna branschens utveckling och händelser. Därtill är medlemskap i Stiftelser och fonder rf en garanti för att i god tid få tillräcklig information om aktuella saker som gäller stiftelser, från förändringar i lagstiftningen och omvärlden till utveckling inom branschen.

Miljörisker

Miljörisker gäller för stiftelsens del dess omvärld samt stiftelsens anställdas och bidragsmottagares hälsa, livs- och arbetsmiljö samt den övriga fysiska miljön.

Ekonomiska risker

Ekonomiska risker handlar om stiftelsens placeringar, solvens, kapital och likviditet. Vissa ekonomiska risker går att förutse, men andra är sådana som stiftelsen själv inte kan påverka. Om stiftelsen ingår i en koncern eller den har dotterbolag, ska stiftelsen identifiera affärsverksamhetens risker, så att affärsverksamheten inte äventyrar genomförandet av stiftelsens syfte. Stiftelsens styrelse ansvarar för att hela stiftelsekoncernen främjar genomförandet av stiftelsens ändamål.

Placeringsrisker

Placeringsrisker utgör en egen kategori, eftersom det krävs specifik planering och särskilt kunnande för att bereda sig på dem. Stipendiestiftelsernas omsorgsfulla medelsförvaltning är en förutsättning för kontinuiteten i deras verksamhet. Den förväntade avkastningen är avgörande för vilken riskprofil stiftelsen är redo att välja. Placeringsprinciperna skrivs för en längre tidshorisont än placeringsplanen, exempelvis med fem års intervaller, och de ska helst också innehålla tydliga principer för hanteringen av placeringsrisker.

Likviditetsrisker

Likviditetsrisker innebär situationer där stiftelsen saknar tillräckligt driftskapital för att betala exempelvis stipendier och löner, trots att stiftelsen i övrigt har tillgångar. Stiftelsen kan undvika likviditetsrisker genom kontinuerlig uppföljning och planering. Stiftelsen ska alltså se till att man i budgeten har tagit

hänsyn till att det finns tillräckligt med likvida medel för de månatliga utgifterna. Därtill ska man reservera en tillräcklig buffert för överraskande kostnader.

Egendomsrisker

Egendomsrisker kan drabba fastigheter, apparater eller annan fast eller lös egendom. Vattenskador, bränder och andra skador orsakade av den yttre miljön är typiska egendomsrisker, mot vilka det går att skydda sig bland annat med försäkringar samt noggranna säkerhets- och räddningsplaner.

Personrisker

Personrisker är risker som antingen riktar sig mot eller orsakas av personalen. Särskilt i en liten stiftelse har personrisker stor betydelse, eftersom det kan påverka hela verksamheten negativt om en nyckelperson säger upp sig eller missbrukar sin ställning. Övriga personrisker kan vara medarbetares sjukdom, olyckor och utbrändhet eller oavsiktliga misstag eller dataläckor. En ovanlig men allvarlig personrisk är missbruk, exempelvis förskingring, som möjliggörs av så kallade farlig arbetskombination. Därtill kan personalens interna relationer orsaka skada för stiftelsens verksamhet. Ett positivt arbetsklimat kan förebygga många risker.

De viktigaste faktorerna att beakta i hanteringen av personrisker är klimatet på arbetsplatsen och arbetets belastning. Stiftelsers verksamhet är sällan olycksbenägen eller farlig, men riskfaktorer bör ändå kartläggas för att förebygga skador eller sjukdom. Att stötta det mentala välbefinnandet är centralt för att förebygga stiftelsers personrisker. Om klimatet på arbetsplatsen är dåligt eller arbetet alltför belastande, kan stiftelsens hela verksamhet utsättas för risker. Ofta återkommande övertid och alltför stora ansvarsområden kan leda till utbrändhet. Stiftelsens bästa metod i hantering av personrisker är att allokera tillräckliga resurser för personalen i form av rätt personaldimensio-nering, kontinuerlig fortbildning, bra arbetshandledning och heltäckande fö-retagshälsovård.

Anseenderisker

Anseenderiskerna hör till de mest betydande för stiftelser. De anknyter i praktiken till alla delar av stiftelsens verksamhet, som kommunikation, öppenhet, rapportering, närståendekretsåtgärder och stipendieprocesserna. Ett gott anseende främjar stiftelsens möjlighet att engagera kompetenta experter och medlemmar i förvaltningsorganen samt få sakkunnig personal och högklassiga ansökningar. Stiftelser med gott anseende får även fler donationer och testamenten. Exempelvis risker för förbjudna närståendekretsåtgärder går enklast att minimera med bra anvisningar och processer för närståendekretsen.

Data- och informationssäkerhetsrisker

Data- och informationssäkerhetsrisker sammanhänger med stiftelsens datasystem och dokument. Sådana risker kan vara exempelvis dataläckage eller att dokument förstörs. Datariskerna omfattar också bland annat att viktig information inte är uppdaterad eller tillgänglig för dem som behöver den. Datasystemens tillräckliga skydd och säkerhetskopiering är nödvändiga för hantering av datarisker. Det är väsentligt att utbilda personalen och fördela ansvaret i datahantering samt informationssäkerhets- och dataskyddsfrågor.

Skaderisker

Skaderisker utgörs av överraskande händelser som sker utanför stiftelsen. Oftast går det att identifiera skaderiskerna, men inte när de eventuellt kan komma att realiseras. Därför ska det bedömas särskilt omsorgsfullt vilken sannolikheten är att skaderiskerna blir verklighet.

Brottsrisker

Stiftelsen kan bli utsatt för brott, såsom stöld, vandalism, bedrägeri eller webbattack. Stiftelsen kan skydda sig mot brott bland annat genom förutseende, övervakning och försäkringar samt genom att omsorgsfullt skydda fast egendom och datasystem.

Avtals- och ansvarsrisker

De största avtalsriskerna anknyter till att stiftelsen och dess partner inte har ingått något avtal eller det är uppgjort slarvigt, exempelvis utan att tydligt definiera ansvarsfördelningen. Ansvarsriskerna gäller sådana ansvar för vilka stiftelsen kan bli ersättningsskyldig. Sådana är exempelvis skador åsamkade andra, som ett GDPR-fel som skadar en stipendieansökare eller miljöskador. Vissa ansvarsrisker är enkla att definiera i förväg, men exempelvis mänskliga misstag som orsakar skadeståndsansvar är svåra att förutse. Det går att bereda sig på ansvarsrisker med bland annat försäkringar och omsorgsfullt uppgjorda avtal som definierar skadeansvar och avtalsbrott.

Beroenderisker

Stiftelsen är förutom många personer även beroende av sina intressegrupper och olika partners. Beroenderiskerna går att hantera genom att sprida användningen av tjänsteleverantörer och undvika avhängighet av en enskild instans eller person.

Övriga risker

Stiftelsens övriga risker kan sammanhänga med exempelvis rättegångskostnader, rekryteringar eller förändringar i regler och lagar.

Metoder för riskhantering

Vissa risker måste man helt enkelt acceptera – men på goda grunder och så att man är medveten om riskens existens. Det primära är alltid att undvika personrisker: människan är det viktigaste i stiftelsernas verksamhet.

Metoder för riskhantering är att reducera, sprida och acceptera riskerna. Det är i praktiken omöjligt att helt och hållet undvika risker, för all verksamhet innebär alltid vissa risker. Genom att reducera risker strävar man efter att påverka sannolikheten för en ogynnsam incident och storleken på dess konsekvenser. Riskreduktion kan till exempel handla om underhåll av system och utrustning samt utbildning av personalen. Å andra sidan är det inte alltid lönsamt att reducera obetydliga risker, om kostnaderna för riskhanteringen överskrider skadorna av själva incidenten.

Försäkringar är det mest kända sättet att överföra risker på någon annans ansvar. Att upphandla olika tjänster och utforma avtal omsorgsfullt kan också minska riskerna. Uppdelning av risken i mindre delar är att sprida risken, och då blir inte heller eventuella påföljder så stora och skadliga. Ett konkret exempel på nyttan med riskspridning är att dela en nyckelpersons uppgifter så att även en annan person vid behov kommer åt samma information och arbeten ifall en personrisk realiseras.

> No risk, no return.

Exempel på stiftelsers riskhanteringsplaner

Yrjö Jahnssonin säätiö (YJS)

YJS riskhanteringsdokumentation består av en tabell för riskkartläggning och en kontinuitetsplan.

Tabell för riskkartläggning

I riskkartläggningstabellen ingår YJS största risker, sannolikheten för att de ska inträffa, följdernas allvarlighetsgrad och åtgärder för att hantera risken. Riskerna är indelade i följande kategorier: personrisker, informationssäkerhets- och dataskyddsrisker, ekonomiska risker, strategiska risker och samhälleliga risker. Tabellens syfte är att ge styrelsen en helhetsbild av vilka stiftelsens största risker är och hur de hanteras.

Kontinuitetsplan

Kontinuitetsplanen är ett konkret dokument att användas av YJS operativa ledning och personal. Planen har tagits fram tillsammans med personalen. Planen innehåller bland annat följande beskrivningar:

- olika funktioners (bl.a. stipendieverksamheten, ekonomiförvaltningen) viktigaste arbetsprocesser, risker och hantering av dem,
- personresurser med ansvarsområden och reserver samt samarbetspartner med kontaktinformation,
- dokumenterade anvisningar (t.ex. systemmanualer, behandlings- och bedömningsanvisningar för stipendieansökningar, kommunikationsplan, arkiveringsinstruktion) samt uppgift om var de finns sparade,
- datasystem och datautrustning med hur långa avbrott de tål samt åtgärder vid störningssituationer i dem och

- instruktioner för ledningen och personalen i olika störningssituationer.

Målet med kontinuitetsplanen är att säkerställa att YJS kritiska funktioner inte äventyras om risker realiseras. Syftet är att försöka säkerställa verksamhetens snabba återstart efter en störning och minska de skadliga effekterna av en sådan för stiftelsen.

Jenny ja Antti Wihurin rahasto

En realiserad risk hindrar eller försvårar det effektiva genomförandet av fonden Jenny ja Antti Wihurin rahastos stadgeenliga syfte helt eller delvis.

Fonden identifierar såväl externa som interna risker som riktas mot den. Vissa av riskerna går att påverka, medan andra beror på exempelvis omvärlden och därmed står utanför stiftelsen påverkansmöjligheter. Man försöker identifiera i synnerhet stora risker och fastställa åtgärder för att hantera riskerna.

Typen av verksamhet som fonden bedriver gör att man måste acceptera somliga risker. Fonden tar rimliga risker (kravet på omsorgsfullhet) i sin placeringsverksamhet och maximala risker i sin stipendieverksamhet med tanke på genomslagskraften efter ansökningarnas bedömning och beviljandet av stipendier.

Riskerna indelas i fyra kategorier: 1. Strategiska, 2. Funktionella, 3. Ekonomiska, 4. Oförutsägbara incidenter. Dessa kategorier inbegriper analys av bland annat följande delområden: förändringar och reglering i omvärlden, genomslaget och anseendet för den stadgeenliga egentliga verksamheten, medelsförvaltning och placeringsverksamhet samt nyckelpersoner.

Jenny ja Antti Wihurin rahastos styrelse fastställer principerna och målen för riskhanteringen samt ansvarar för att de godkänns och övervakas. Kapitalförvaltningskommittén bereder uppdateringar av riskhanteringsprinciperna och riskanalys för styrelsen på föredragning av ombudet.

Riskhanteringsprinciperna och riskanalysen behandlas och uppdateras vid behov på styrelsens årsmöte.

En regelbunden bedömning av fondens risker utförs av den operativa ledningen. Den operativa ledningen rapporterar betydande potentiella eller inträffade avvikelser i fondens anseende, genomslag och ekonomi till styrelsen och kapitalförvaltningskommittén på möten och vid behov även annars. Kapitalförvaltningskommittén och ombudet rapporterar sannolika eller realiserade betydande risker till fondens styrelse.

Turun yliopistosäätiö

Stiftelsen Turun yliopistosäätiö har i sin planering kombinerat compliancefunktionen, riskhanteringen och kontinuitetsplaneringen. Den stora helheten har indelats enligt de olika delområdena i stiftelsens verksamhet till en praktisk checklista. Avsikten är att ge en så gott som heltäckande överblick av stiftelsens verksamhet samt arbets- och ansvarsfördelning. De detaljerade uppgiftsförteckningarna och ansvarsfördelningen underlättar såväl planeringen av det dagliga arbetet som utvärdering på längre sikt.

Modellen bidrar till att säkerställa att stiftelsen gör allt som bör göras. Den används för att avtala stiftelsens interna arbetsfördelning, vad respektive medarbetare och styrelsen ansvarar för, överföra information till anställda och nya förtroendevalda samt följa upp arbetsmängden och behovet av vikarier. Därtill hjälper modellen styrelsen och revisorn att följa upp stiftelsens verksamhet i detalj och därmed uppfylla sin övervakningsplikt.

COMPLIANCE-CHECKLISTA FÖR STIFTELSER

BASERAD PÅ KONTKANEN (2020)

1. STRATEGI OCH VERKSAMHETSBERÄTTELSE

- Kraven i stiftelselagen och rekommendationerna i *God förvaltning i stiftelser*, ledningens prognostiserings- och riskhanteringsarbete

2. FÖRVALTNINGSORGAN

- Bindningar, vetenskapliga experter, efterträdarplanering
- Dokumentering: regelefterlevnad, mandatperioder, antal och representation, i tur att avgå
- Anmälningar till Stiftelseregistret
- Närståendekretsanmälningar

3. EKONOMIFÖRVALTNING

- Rapporteringssystem: på vilken nivå, hur, till vem och hur ofta görs rapporter?
- Resultatrapport, kassarapport och stipendierapport
- Rapporter i anknytning till upphandling
- Undvikande av farliga arbetskombinationer (kedjan för anskaffning och godkännande sköts alltid av flera personer)
- Revisionsberättelse, genomförande av revisionen och förvaltningsrevision (processbeskrivning, ansvarsfördelning)
- Uppdaterade system
- Koncerninstruktioner

4. PERSONAL

- Anställningsavtal
- Lönebetalningens organisation
- Arbetarskyddsfrågor, samverkan, efterlevnad av arbetslagstiftningen (uppföljning av semestrar och arbetstid)
- Företagshälsovård, förmåner, person- och ansvarsförsäkringar (olycksförsäkringar osv.)

5. SKYDD AV EGENDOMEN

- Egendoms- och andra försäkringar

- Serviceböcker
- Räddningsplaner
- Inventarieförteckning
- Inbrotts- och larmsystem

6. PLACERINGSTILLGÅNGAR

- Uppföljningsrapporter över placeringar
- Kapitalförvaltningsavtal
- Konsult- och andra avtal
- Uppdragens start och verkställighet
- Kontroll av befogenheterna (köp och försäljning)

7. FASTIGHETSTILLGÅNGAR

- Hyresavtal och kontroll av dem
- Säkerställande av fastighetsbolagens verksamhet
- Fastighetsutvecklingsprojekt
- Anskaffningar

8. BESKATTNING

- Uppfyllande av kraven på allmännyttighet
- Donationers och stipendiers beskattning
- Mervärdesskatt (fastigheter)
- Fastighetsskatt
- Placeringarnas skattefrågor
- Beskattning av fastighetsinkomster
- Utnämningsbeslut
- Återbäring av källskatt (utdelning från utlandet)

9. TESTAMENTEN, DONATIONER OCH FONDER

- Villkor i testamenten och donationer (t.ex. gravskötselavtal)
- Efterlevnad av fondernas regler, förvaltningsnämnd
- Fondprospekt

10. GÄLLANDE EXTERNA AVTAL

- Kontorsapparater (kopiator, videokanon osv.)
- IT- och kommunikationstjänster
- Renhållning
- Avtalsprocesser (upphandling och dess regler)

11. HÅLLBARHET

- Socialt ansvar
- Miljöfrågor
- Förvaltningsansvar, corporate governance

12. INFORMATIONSSÄKERHET OCH DATASKYDD

- Efterlevnad och övervakning av dataskyddsförordningarna
- Informationssäkerhet i systemen och verksamheten

13. STIPENDIER

- Processbeskrivning
- Regler, jäv
- Expertinstruktioner
- Beslut, utbetalning och återbetalning
- Rapportering och annan övervakning
- Lagstadgade meddelanden om stipendier (LPA, skattemyndigheterna)

14. KOMMUNIKATION

- Kommunikationsplan och ansvarsfördelning enligt uppgift
- Krissituationer

> Effekten av god riskhantering kan ge mycket större mervärde än bara beredskap för skadliga situationer.

ALLMÄN MALL FÖR RISKHANTERINGSPLAN

Riskens sannolikhet

1. Osannolik
2. Möjlig
3. Sannolik

Riskens allvarlighetsgrad

1. Låg
2. Skadlig
3. Allvarlig

Identifierad risk	Riskens sannolikhet	Riskens allvarlighetsgrad	Riskhanteringsåtgärder	Ansvarsfördelning
1. STRATEGISKA				
Målen uppfylls inte	1–3	1–3	Kontinuerlig uppföljning av att strategin och verksamhetsplanen uppfylls, regelbunden utvärdering av genomslagskraften	Styrelsen, VD, revisor
Samhälleliga och politiska risker	1–3	1–3	Medlemskap i SF, aktiv kommunikation	Styrelsen, VD
Anseenderisker	1–3	1–3	Ansvarsfull verksamhet, strategi och praxis för kommunikationen, medlemskap i SF	VD, styrelsen, kommunikationsdirektören
Ansvarsrisker	1–3	1–3	Efterlevnad av God stiftelsepraxis, beaktande av ESG-perspektiv	Styrelsen, VD
...	1–3	1–3		
2. OPERATIVA				
Personrisker	1–3	1–3	Bra personalpolitik, proaktiva åtgärder för arbetstrivsel, system med reservpersoner, fortlöpande utbildning	VD, styrelsen
Datasystemsrisker	1–3	1–3	Uppdaterade uppföljnings- och övervakningsprocesser, dokumentering av användningen	VD, expertkonsultation
Informationssäkerhetsrisker	1–3		Efterlevnad av GDPR-reglerna, avtal, utbildning, revisioner	VD, styrelsen
Ansvars- och avtalsrisker	1–3	1–3	Processer för avtalsuppföljning, ansvarsförsäkringar, avtalsregister	VD, styrelsen
...	1–3	1–3		

Identifierad risk	Riskens sannolikhet	Riskens allvarlighetsgrad	Riskhanterings-åtgärder	Ansvarsfördelning
3. EKONOMISKA				
Placeringsrisker	1–3	1–3	Uppdaterad placeringspolicy, riskanalyser, spridning	Styrelsen, VD, revisor
Likviditetsrisker	1–3	1–3	Kassaflödesplanering, rapporteringssystem	VD, ekonomidirektören
Egendomsrisker	1–3	1–3	Rapporteringssystem, försäkringar	Styrelsen, VD, ekonomidirektören
...	1–3	1–3		
4. ÖVRIGA				
Stipendiemottagarens missbruk	1–3	1–3	Utveckling av finansieringens uppföljning	VD, hela samfundet
Personalens eller förtroendevaldas missbruk	1–3	1–3	Personalpolitik, processer för internrevision, undvikande av farliga arbetskombinationer	Styrelsen, VD, ekonomidirektören, revisor
...	1–3	1–3		

”Revisionens och tillsynens perspektiv:
det som inte har dokumenterats har inte gjorts.

Läs mer

Harjula, R. – Kela, O. – Löfman, M. – Maijala, T. – Perälä, S. – Suvikumpu, L. – Tikka, P., *Förslag till förfaringssätt gällande närståendekretsen för stiftelsens ledning och revisorer*. Stiftelser och fonder rf, 2018. https://saatiotrahastot.fi/wp-content/uploads/2020/01/srnk_lahipiiriohje-pa-svenska_valmis_web.pdf

Hopkin, Paul, *Fundamentals of risk management. Understanding, evaluating, and implementing effective risk management.* Kogan Page Ltd 2017.

God stiftelsepraxis. Stiftelser och fonder rf, 2020. https://saatiotrahastot.fi/wp-content/uploads/2020/05/God-stiftelsepraxis.pdf

Jauhiainen, Jyrki – Kaisanlahti, Timo – Kela, Oili, *Säätiölaki*. Kauppakamari 2017.

Kontkanen, Jaakko, *Apurahasäätiöiden compliance eri sidosryhmien näkökulmasta*. Pro gradu, laskentatoimi ja rahoitus, Turun yliopisto 2020. http://urn.fi/URN:NBN:fi-fe2020112092243

Kuusela, Hannu – Ollikainen, Reijo (red.), *Riskit ja riskienhallinta*. Tampere University Press 2005. https://trepo.tuni.fi/bitstream/handle/10024/65418/riskit_ja_riskienhallinta_2005.pdf?sequence=1

Löfman, Martin – Tikka, Päivi – Suvikumpu, Liisa, *God informationshantering i stiftelser.* Stiftelser och fonder rf, 2018 (uppdaterad 2019). https://saatiotrahastot.fi/sv/god-informationshantering-i-stiftelser/

Maijala, Terhi, *Huolellisuusvelvollisuus säätiössä*. Alma Talent 2021.

Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf

Pykäläinen-Syrjänen, Ritva, *Säätiön tehokkuus. Corporate Governance -säännösten vaikutuksesta säätiön tarkoituksen tehokkaaseen toteuttamiseen*. WSOYpro 2007.

Ratsula, Niina, *Compliance. Eettinen ja vastuullinen liiketoiminta*. Talentum 2016.

ISO 31000 Riskienhallinta. Suomen Standardisoimisliitto SFS ry 2018. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/3/652941.html.stx.

Suvikumpu, Liisa (red.), *God förvaltning i stiftelser*. Stiftelser och fonder rf, 2015. https://saatiotrahastot.fi/wp-content/uploads/2020/01/srnk_god-forvaltning-i-stiftelser_screen.pdf

Stiftelselagen 487/ 2015. https://www.finlex.fi/sv/laki/alkup/2015/20150487