Österbottens välfärdsområde
Pohjanmaan hyvinvointialue

Anvisning för intern kontroll och riskhantering

Välfärdsområdesstyrelsen 4.5.2026 § 115

Innehållsförteckning

1. Inledning

Grunderna för intern kontroll och riskhantering har fastställts i det dokument som godkänns i välfärdsområdesfullmäktige. Denna anvisning kompletterar välfärdsområdets grunder för intern kontroll och riskhantering. Ytterligare så innefattar de ägarpolitiska linjedragningar som godkänts i fullmäktige bestämmelser om kontrollaktiviteter och rapportering som hänför sig till ägarstyrning.

Syftet med anvisningen om intern kontroll och riskhantering är att förenhetliga de tillvägagångssätt som anknyter till intern kontroll men också att säkerställa att överenskomna och godkända tillvägagångssätt och anvisningar tillämpas. Välfärdsområdets anvisning om intern kontroll och riskhantering gäller organisationens samtliga organ, ledning och personer i förmansställning samt i bred bemärkelse hela personalen.

Vid beredningen av anvisningen har man iakttagit de bestämmelser i välfärdsområdeslagen (611/2021) som berör intern kontroll och riskhantering. Därutöver har man vid beredningen av anvisningen tillgodogjort internationella standarder för intern kontroll (COSO ERM) och riskhantering (ISO 31000).

2. Mål och verksamhetsprinciper för intern kontroll och riskhantering

2.1 Mål för intern kontroll och riskhantering

Målet med den interna kontrollen och riskhanteringen är att säkerställa att verksamheten bedrivs effektivt resultatrikt och legitimt samt att rapporteringen är tillförlitlig. Legitim verksamhet innebär att gällande lagstiftning och god förvaltningssed tillämpas i organisationens verksamhet och beslutsfattande. Resultatrik verksamhet innebär att uppställda strategiska och verksamhetsmässiga mål uppnås inom ramen för den budget som godkänts i fullmäktige. En resultatrik verksamhet innebär också att verksamheten är verkningsfull att de tjänster som tillhandahålls är kvalitativa. Med tillförlitlighet i rapporteringen avses att den ekonomiska och övriga rapporteringen är korrekt och aktuell.

Intern kontroll och riskhantering stödjer ledningen i styrningen av verksamheten.

2.2 Verksamhetsprinciper och delfaktorer som hänför sig till intern kontroll och riskhantering

I samband med ledning och ordnande av förvaltning är välfärdsområdesstyrelsen och styrelsen underställda organ, organisationens verksamhets- och resultatområden ålagda att hörsamma organisationens värden och etiska principer, uppställda mål, att fastställa

övervakningsansvar, att ordna och utveckla den interna kontrollen och riskhanteringen samt att se till att personalen är kompetent.

Med hjälp av riskbedömningar identifierar, bedömer och analyserar organisationens verksamhets- och resultatområden de risker som äventyrar de strategiska, verksamhetsmässiga och ekonomiska målen på organisationsnivå, med beaktande av de förändringar som sker i verksamhetsmiljön, befintliga riskhanteringsåtgärder, risker för oegentligheter samt förändringar som i avsevärd grad kan påverka det interna kontrollsystemet.

Med hjälp av kontrollåtgärder främjar organisationens verksamhets- och resultatområden måluppfyllelsen, bekräftar att riskhanteringsåtgärder blir vidtagna samt att de tillvägagångssätt som hänför sig till förvaltning och ekonomi är vederbörliga. Kontrollåtgärder som minskar risker är exempelvis befogenheter, planer, anvisningar, processbeskrivningar, rapporteringsrutiner samt olika ekonomiska och administrativa kontrollmekanismer, arbetsfördelningar och systemkontroller.

För att bistå den interna kontrollen utarbetar och anskaffar organisationens verksamhets- och resultatområden högklassig och relevant information för ledningen om hur den interna kontrollen och riskhanteringen fungerar. Ledningen upplyser personalen om de mål och befogenheter som uppställts för den interna kontrollen och riskhanteringen samt samarbetar med utomstående aktörer i frågor som påverkar ändamålsenligheten i den interna kontrollen och riskhanteringen.

Organisationens verksamhets- och resultatområden utvecklar, uppföljer och bedömer ständigt den interna kontrollen och riskhanteringen samt genomför varierande utvärderingar för att säkerställa att samtliga delfaktorer som anknyter till intern kontroll och riskhantering är i bruk och fungerar. Organisationens verksamhets- och och resultatområden upplyser i tid de aktörer som ansvarar för att korrigerande åtgärder blir vidtagna om förekommande brister i den interna kontrollen och riskhanteringen, och vid behov även organisationens ledning och styrelse.

3. Intern kontroll och riskhantering som en del av god ledning och förvaltning

3.1 God förvaltnings- och ledningssed samt principer för god förvaltning

Med hjälp av intern kontroll och riskhantering säkerställer man att verksamheten sköts enligt god lednings- och förvaltningssed. Med god förvaltnings- och ledningssed avser man det redovisningsskyldighets- och ansvarssystem som används för att styra

verksamhet och ekonomi och som bidrar till tillförlitligheten, effektiviteten och transparensen i förvaltningen och serviceproduktionen. Systemet grundar sig på organisationens värden, klienternas och invånarnas behov samt utvärderingar av verksamhetsresultatet. Det väsentliga är att man gör linjedragningar som är till för att trygga förutsättningarna för en resultatrik verksamhet men som samtidigt bemöter de krav som ställs på en etisk och ansvarsfull verksamhet. I det här sammanhanget framhävs förtroendevaldas, förmäns och anställdas skyldighet att ärligt och uppriktigt följa gällande lagar och stadgor samt ledningens bestämmelser.

I välfärdsområdets verksamhet ska man följa de principer som fastställts för god förvaltning. De uppgifter som hör till organisationens kompetens ska utföras med beaktande av medborgarnas rättsskydd och i övrigt på ett sakligt och förtroendeingivande sätt. De centrala principerna som gäller för god förvaltning inom den offentliga förvaltningen är de rättsprinciper som fastställs i förvaltningslagen (434/2003), dvs. likställighet, ändamålsbundenhet, objektivitet, proportionalitet och skydd för berättigade förväntningar. Till grunderna för god förvaltning hör också service principer och adekvat service, rådgivningsskyldigheter, kravet på gott språkbruk och kravet på samarbete mellan myndigheter.

Lagen om tjänsteinnehavare i kommuner och välfärdsområden (304/2003) förutsätter att tjänsteinnehavaren utför de uppgifter som hör till tjänsteförhållandet utan dröjsmål och på behörigt sätt. Tjänsteinnehavaren ska uppträda så som hans eller hennes ställning och uppgift förutsätter. Om motsvarande föreskrifter som rör arbetstagare stadgas i arbetsavtalslagen (55/2001).

3.2 Lednings- och styrningssystemet

Välfärdsområdets organisation och befogenhetsförhållanden fastställs i förvaltningsstadgan. Närmare bestämmelser kan ges i verksamhetsstadgan.

Fullmäktige är organisationens högsta beslutande organ. Fullmäktige svarar för det strategiska beslutsfattandet och för de mål som ställs upp för hela organisationen, för balansen mellan ekonomi och verksamhet samt för utvärderingen och uppföljningen av verksamheten. Under fullmäktige lyder revisionsnämnd vars uppgift är att bedöma huruvida de mål för verksamheten och ekonomin som fullmäktige satt upp har nåtts i och huruvida verksamheten är ordnad på ett resultatrikt och ändamålsenligt sätt samt bedöma hur balanseringen av ekonomin utfallit.

Styrelsen leder organisationen och ansvarar för organisationens förvaltning och ekonomi. Under styrelsen lyder en individsektion, en ägarstyrningssektion, en personalsektion, en sektion för räddningsväsendet, en sektion för främjande av

välbefinnande och hälsa och kontaktytor samt nationalspråksnämnden och välfärdsområdesvalnämnden. Organisationens direktör, som är underställd styrelsen, svarar för verksamheten i hela organisationen samt för ledning och utveckling.

De linjedragningar och tillvägagångssätt med vilka man kan styra organisationens verksamhet så att man en får en rimlig säkerhet om att de uppställda målen har uppnåtts samt för att verksamheten bedrivs lagenligt, etiskt och ansvarsfullt samt att rapporteringen är tillförlitlig är centrala för en god lednings- och förvaltningssed.

Följande delfaktorer är centrala för ordnandet och ledningen av förvaltningen:

- gällande lagstiftning
- förvaltningsstadgan och organisationsstrukturen
- värden och etiska principer
- ledningens tillvägagångssätt och delegering av kompetens
- principer för personalledning
- yrkeskompetens och incitament
- det ömsesidiga förhållandet mellan förtroendevalda och tjänstemannaledningen
- informationsutbytet

3.3 Kontroll- och övervakningssystemet

Genom kontroll och övervakning skapar man förutsättningar för att organisationen ska kunna uppnå sina mål. Kontrollaktiveter förebygger också risker som hänför sig till ekonomi och verksamhet. Vid övervakningen av organisationens förvaltning och ekonomi bildar den externa revisionen och utvärderingen samt den interna kontrollen ett vittomfattande övervakningssystem. Välfärdsområden är skyldiga att ordna en oberoende internrevision av området, vars uppgift är att bedöma hur väl den interna kontrollen fungerar.

Den externa revisionen och utvärderingen ska organiseras så att den är oberoende av den operativa ledningen. Enligt välfärdsområdeslagen svarar revisionsnämnden och revisorn för denna verksamhet. Revisionsnämnden utvärderar organisationens strategi och huruvida de övriga mål som fullmäktige uppställt har uppnåtts. Revisorn svarar för granskningen av förvaltningen och ekonomin.

Den interna kontrollen bistår ledningen och hjälper till med hanteringen av risker. I enlighet med den förvaltningsstadga som godkänts av fullmäktige svarar styrelsen för ordnandet av den övergripande interna kontrollen och riskhanteringen. Den operativa

ledningen igen svarar för att intern kontroll och riskhantering verkställs och för dess resultat inom det egna verksamhetsområdet och resultatområdet.

3.4 Definition av mål för den interna kontrollen

Med den interna kontrollen avses interna förfaranden och verksamhetsmetoder genom vilka ledningen strävar efter att trygga verksamhetens lagenlighet och resultat. Intern kontroll omfattar organisationens samt dess ansvarsområdens och serviceområdens egen kontroll som genomförs av ledningen eller på ledningens vägnar. Genom den interna kontrollen synar man hur och på vilka sätt ledningen bekräftar att målen inom det egna ansvarsområdet eller inom den egna verksamhetsenheten blir uppnådda, att verksamheten tillhandahålls inom ramen för lagar, bestämmelser, anvisningar och beslut, att resurser används effektivt och framgångsrikt, att egendomen är tryggad och att ledningen får adekvat, ändamålsenlig information i rätt tid. Den interna kontrollen utgör en väsentlig del av styrningen och ledningen av den verksamhet som tillhandahålls varje dag.

En grundläggande förutsättning för att ledningen ska kunna vara framgångsrik är att ledaren har tillgång till aktuell information om läget inom det område eller den enhet som den leder för att ledningen av verksamheten inte ska grunda sig på bara antaganden. På allmän nivå är målet med den interna kontrollen att förbättra kostnadseffektiveten, att ordna en högklassig och transparent förvaltning samt att säkerställa att arbetet är meningsfullt. Här är det alltså fråga om en självvärdering av verksamheten där målet är att ständigt förbättra verksamheten.

Mera detaljerat kan målsättningarna för den interna kontrollen fördelas enligt följande:

Effekt och resultat. Genom kontroll bekräftar man att uppställda mål har uppnåtts, att produkter och tjänster håller kvaliteten samt att verksamheten tillhandahålls ekonomiskt och produktivt.

Rapportering och säkerställande av uppgifter: Genom tillsyn sörjer ledningen och förmännen för att deras ansvarsområden tillhandahåller och upprätthåller tillförlitliga uppgifter om verksamheten, ekonomin och förvaltningen. Uppgifterna ska rapporteras korrekt och tidsenligt.

Verksamhetens lagenlighet och hörsammandet av ledningens anvisningar. Genom tillsyn bekräftar man att lagar och förordningar samt organisationens beslut, regler och anvisningar följs.

Tryggande av resurser och egendom. Genom kontrollen bekräftar man att organisationens resurser används förståndigt och ekonomiskt till organisationens godo och att resurserna skyddas mot förluster som beror på misstag, dålig skötsel, misshushållning, missbruk, bedrägerier eller annan regelvidrig verksamhet.

Naturen, innehållet och omfattningen av verksamheten samt verksamhetsenhetens ekonomi och de risker som är förknippade med den påverkar den interna kontrollen. Kontrollen är tillräcklig då verksamheten är ordnad så att det finns en rimlig säkerhet om att uppställda mål uppnås. Kontrollåtgärderna måste vara ekonomiska och effektiva. Den interna kontrollen inrymmer organisationens egen verksamhet samt verksamhet som organisationen ansvarar för genom ägande, styrnings- och tillsynsansvar samt med stöd av andra skyldigheter eller avtal.

3.5 Definitioner av och målet med riskhantering

Riskhantering är ett systematiskt och proaktivt sätt att säkerställa att organisationens mål uppnås och att verksamheten kan fortgå oavbrutet och utan störningar. Genom att identifiera, analysera och hantera verksamhetsrelaterade hot och möjligheter får organisationen en rimlig säkerhet om att både ekonomiska och verksamhetsmässiga målsättningar kan uppfyllas och att dess anseende skyddas.

En risk definieras som en potentiell händelse eller händelsekedja som på kort eller lång sikt kan äventyra måluppfyllelsen, påverka organisationens verksamhet negativt eller hota dess rykte. Risk kan också innebära att en potentiell möjlighet inte realiseras trots att resurser finns tillgängliga. Att förstå och bedöma både risker och möjligheter är därför centralt.

Riskhanteringen är en integrerad del av planering, beslutsfattande och uppföljning i organisationens löpande verksamhet. Den är inbäddad i processer och arbetsmetoder och kopplas bland annat till de årligen återkommande planerings- och rapporteringscyklerna för verksamhet och ekonomi.

Som stöd finns en riskhanteringshandbok som ger mer detaljerade anvisningar om ansvarsfördelning, arbetsgång och rapporteringsrutiner. På så sätt säkerställs att riskbedömning och rapportering genomförs på ett enhetligt och strukturerat sätt.

En övergripande riskhantering är också en del av organisationens interna kontroll. Genom kartläggning och bedömning av risker får det interna tillsynssystemet tillgång till aktuell information, vilket gör det möjligt att anpassa åtgärder efter förändringar i verksamhet och omvärld.

4. Kontrollåtgärder

4.1 Planering, val och förverkligande av kontrollåtgärder

Kontrollåtgärder syftar till att främja och säkerställa måluppfyllelsen genom att minska riskerna till en acceptabel nivå. Med hjälp av kontrollåtgärder kan man bekräfta att fastställda tillvägagångssätt och instruktioner följs samt att åtgärder vidtas för att hantera risker.

Ledningen ansvarar för att kontrollansvaret är tydligt fastställt och att förmännen är sakkunniga samt agerar i enlighet med de bestämda rutinerna och instruktionerna. Förmännen ansvarar för att personalen är medveten om dessa rutiner och instruktioner, samt för att varje medarbetare förstår sin roll och sina uppgifter i genomförandet av kontrollåtgärderna. Vissa kontrollåtgärder kan innebära att ledningen endast lämnar begränsad information till personal eller externa parter.

Förmännen genomför kontrollåtgärderna noggrant, verifierar att de är korrekt utförda och vidtar vid behov korrigerande åtgärder. Valet och utvecklingen av kontrollåtgärder påverkas av verksamhetens art, omfattning och komplexitet, verksamhetsmiljön och förändringar i den, i vilken grad teknologi används samt beroendet av datasystem.

Övervakningsåtgärder planeras utifrån ett riskperspektiv, där nyttan med åtgärderna vägs mot de kostnader de medför. En stor del av kontrollåtgärderna genomförs inom ramen för de rutiner och säkerställande åtgärder som ingår i personalens dagliga arbete.

Ledningen och förmännen ska årligen, vid bokslut och vid behov, se över kontrollåtgärdernas aktualitet och uppdatera dem vid behov. Kontrollåtgärder kan också kompletteras eller omformas utifrån riskbedömningar, så att fokus ligger på de risker som bedöms vara mest betydande.

4.2 Naturen av kontrollåtgärderna

Med hjälp av de förebyggande kontrollåtgärderna som bakats in i verksamheten och datasystemen kan man upptäcka och förhindra eller korrigera fel som uppdagas i processer, hanteringen av händelser eller uppgifter.

Den kontroll som inbakats i verksamhetsprocesser och datasystem omfattar kontrollmekanismer som:

- stöder hörsammandet av lagar, beslut samt bestämda tillvägagångssätt och anvisningar
- stöder riktigheten i processförloppet och användningen av datasystem
- övervakar att befogenheter hörsammas

- säkerställer riktigheten i händelser och uppgifter
- skyddar information
- förhindrar misstag och missbruk
- säkerställer att uppgifter är tillräckligt differentierade
- tryggar kontinuiteten i verksamheten

Här nedan följer exempel på kontrollåtgärder som planerats för att uppdaga misstag och avvikelser:

- uppföljning av uppfyllelsen av ekonomiska mål
- analysering och uppföljning av rapportering
- uppföljning av verksamheten och avvikelser i denna
- varierande, regelbundna kontroll- och avstämningsmekanismer
- uppföljning och rapportering av överenskomna risknivåer
- byte av uppgift
- fysiska och tekniska kontrollåtgärder

Syftet med de korrigerande kontrollåtgärderna är att understöda utredningen och korrigeringen av misstag. En korrigerande kontrollåtgärd kan exempelvis innebära att man bekräftar eller återställer uppgifter eller tillgodogör sig av felstatistik.

4.3 Användning av datasystem vid kontroll

Kontrollåtgärderna och datatekniken är kopplade till varandra på två sätt. När processerna i organisationen omsätts i praktiken med hjälp av ett eller flera datasystem behövs det kontrollåtgärder som hänför sig till datasystemen och de risker som är förknippade med användningen av dessa datasystem. Å andra sidan kan man antingen helt eller delvis använda dessa datasystem för att förverkliga de kontrollåtgärder som behövs för att tillse processen eller handläggningen av händelser. I de flesta processer förverkligas kontrollen som en kombination av automatiserade kontrollåtgärder och kontrollåtgärder som genomförs av människor (t.ex. uppföljningen av budgeten).

I processer som tillgodogör sig av datasystem är det i allmänhet effektivast att förverkliga kontrollåtgärderna med hjälp av datasystem. Vid användning av datasystem kan man bland annat ty sig till följande kontrollåtgärder:

- fastställande av användarrättigheter och olika nivåer av befogenheter
- logguppgifter över händelser och informationshantering samt möjlighet att spåra förändringar
- kontroll av inmatade uppgifter
- andra programrelaterade kontroller och avstämningar

- säkerhetsklassificeringar och skydd av uppgifter
- uppföljning och rapportering av fel och avvikelser
- kontroll av användningen av systemen, bland annat med hjälp av logguppgifter

Ägare av datasystem och förmän svarar för att dylika kontrollåtgärder ordnas, för övervakningen av att dessa åtgärder fungerar samt för att brister i kontrollen uppföljs, rapporteras och korrigeras. Genom en avgränsning av användarrättigheterna kan man se till att uppgifterna blir effektivt differentierade. Datasystemen kan inte alltid förses med tillräckligt automatiserade kontrollmekanismer, varför förmannen i dylika lägen måste se till att man vidtar ersättande kontrollåtgärder och övervakar att dessa åtgärder fungerar.

Datatekniken måste aktivt uppföljas för att problemen ska uppdagas och för att man ska kunna vidta korrigerande åtgärder. Det måste finnas processer för hur IKT-funktioner utvecklas, används och underhålls, samtidigt bör man se till att det finns kontrollåtgärder för IKT-processerna med vilka man kan hantera karaktäristiska risker.

De allmänna kontrollåtgärderna som förverkligas inom ramen för organisationens IKT-verksamhet bidrar till att man kan bekräfta att informationshanteringen är integrerad, felfri och tillgänglig. Målet med de allmänna kontrollåtgärderna som hänför sig till IKT-processerna är att övervaka den datatekniska miljön, tillgängligheten till datatrafiknät och datasystem samt upphandlingen och underhållet av programvaror och apparater. Med tanke på riktigheten av uppgifterna i systemen utgör förändringshantering och hanteringen av användarrättigheter de viktigaste, allmänna IKT-kontrollmekanismerna.

För att upprätthålla de datatekniska funktionerna behövs det säkrings- och återställningsrutiner samt kontinuitets- och återhämtningsplaner som är avhängiga av de risker och följder som anknyter till ett eventuellt driftsavbrott. När ovanstående uppgifter eller en del av dessa uppgifter sköts av utomstående IKT-leverantörer måste organisationens informationsförvaltning se till att rutinerna fungerar och ingå avtal om riskhantering och tillse dessa avtal. I dessa avtal ska styrning, övervakning och eventuell granskningsrätt av tjänster som tillhandahålls av dylika leverantörer tas i beaktande.

4.4 Identifiering och förebyggande av farliga arbetskombinationer

Identifieringen av farliga arbetskombinationer bygger på processbeskrivningar och bedömningen av de risker som är förknippade med processerna. Om en person ensam handlägger en hel händelsekedja eller flera delar av en kedja i en process som är utsatt för oegentligheter och fel så är det fråga om en farlig arbetskombination. En farlig arbetskombination möjliggör oegentligheter eller allvarliga fel som kan bli förbisedda.

För att undvika fel och oegentligheter ska befogenheter och uppgifter uppdelas, dvs. differentieras, så att händelser exempelvis godkänns och dokumenteras och medel sköts av olika personer. Farliga arbetskombinationer kan förekomma förutom inom ekonomiförvaltningen, inköps- och materialförvaltningen även inom andra verksamheter i organisationen, såsom i samband med informationshantering.

Verksamhet där det inte finns flera anställda är förknippad med en större risk för att det ska uppstå farliga arbetskombinationer. Om det inte är möjligt att fördela uppgifterna mellan flera personer ska man använda sig av efterkontroll för att bekräfta riktigheten i verksamheten. Exempelvis så att förmannen i efterskott godkänner vidtagna åtgärder och händelser på ett sätt som gör det möjligt att påvisa godkännandet också senare.

För att säkerställa att differentieringen av arbetsuppgifterna ska bli omsatt i praktiken är det också viktigt att se till att arbetstagaren inte har för omfattande användarrättigheter till datasystem i förhållande till sina arbetsuppgifter.

4.5 Anmälning, identifiering och bekämpning av oegentligheter

Ohederliga, oetiska eller avsiktliga handlingar som bryter mot lagar eller organisationens anvisningar anses som oegentligheter.

Målet med den interna kontrollen är att radera möjligheterna för att man ska kunna begå oegentligheter. Om oegentligheter ändå begås så uppdagas oegentligheterna av en ändamålsenligt fungerande intern kontroll. Ledningen svarar för att den interna kontrollen fungerar och är ålagd att ingripa i uppdagade oegentligheter. När det gäller oegentligheter har organisationen nolltolerans.

Misstanke om oegentlighet kan uppstå i samband med kontrollåtgärder, som ett resultat av en granskning, utomstående angivelse eller via andra källor.

Kännetecken på oegentligheter är exempelvis följande:

- bestämmanderätt har använts i strid mot anvisning eller delegerad befogenhet
- felaktiga handlingar eller handlingar som misstänks vara förfalskade
- handlingar eller egendom som har förstörts eller misstänks ha försvunnit
- misstanke om vilseledande av person
- missbruk av bestämmanderätt gentemot underställda

Personalen ska rapportera tecken på eventuella oegentligheter eller förseelser i första hand till sin förman. En anmälan kan vid behov även göras till organisationens direktör eller förvaltningsdirektören men kan även göras via organisationens anmälningskanal (en länk till kanalen finns på intranätet: Framsida ->Mitt välfärdsområde -> Förvaltning ->

Etisk rapporteringskanal). Det hör primärt till närchefens uppgift att utreda uppdagade oegentligheter. Organisationens ledning kan efter eget omdöme ta in en utomstående aktör för att göra en intern revision i syfte att utreda oegentligheter.

5. Riskhantering

5.1 Perspektiv och dimensioner som hänför sig till riskhantering

Riskhantering genomförs på alla organisationsnivåer, i olika funktioner och processer. Dessutom ska serviceproducenter som tillhandahåller utlokaliserade tjänster omfattas av en tillräcklig riskhantering. Riskhanteringsperspektiven omfattar strategiska och ekonomiska risker, verksamhetsrelaterade risker och externa risker.

Styrelsen ansvarar för riskhanteringen och samordningen av den samt bestämmer om försäkring av organisationens egendom och ansvar. Respektive verksamhetsområde måste vara medvetet om och kartlägga de risker som inverkar på den egna verksamheten (i synnerhet finansierings-, personal-, egendoms- och verksamhetsrisker) samt vidta åtgärder med vilka dessa risker kan förebyggas eller avge ett förslag till styrelsen om dessa.

I organisationen har man delat in riskhanteringen i tre delar baserat på de olika processerna: strategiska, operativa och förändringsrisker.

5.2 Strategiska och ekonomiska risker

Organisationens måluppfyllelse, val och beslut är förknippade med risker som kallas strategiska och ekonomiska risker. I samband med bedömningen av de strategiska och ekonomiska riskerna måste organisationen bestämma hurdana risker den är beredd att ta. I samband med bedömningen av dessa risker kan man ofta identifiera och tillgodogöra möjligheter.

Välfärdsområdets strategiska mål och åtgärder har fastställts i organisationens strategi. I samband med budgetarbetet och motsvarande processer fastställer verksamhetsområden sina verksamhetsmässiga och ekonomiska mål som är härledda från organisationens strategiprogram. Man identifierar de risker som kan äventyra måluppfyllelsen och konsekvenserna av dessa risker samt uppgör och uppdaterar planer och åtgärder som behövs för att hantera dessa risker. Fullmäktige beslutar om bindande och övriga verksamhetsmässiga mål som omfattas av budgeten.

Med ekonomiska risker avser man i det här sammanhanget närmast val och risker som är förknippade med organisationens hushållning, likviditet, finansiering och placeringar. De val och beslut samt de risk- och möjlighetsanalyser som görs i anslutning till dessa är av central vikt i fråga om de strategiska och ekonomiska riskerna.

5.3 Verksamhetsrelaterade risker

Verksamhetsrelaterade risker är risker som är förknippade med organisationens personal, verksamhet och legitimitet, processer samt uppgifter och datasystem som i regel medför skadliga konsekvenser. Verksamhetsriskerna är av olika karaktär på olika nivåer av verksamheten. På individ och enhetsnivå handlar det om riskerna i den dagliga verksamheten och en god säkerhetskultur där varje arbetstagare vågar lyfta upp risker är grunden för en säker verksamhet. På resultatområdesnivå handlar verksamhetsrelaterade risker mera om processrisker men också om att sprida god praxis och riskmedvetenhet över enhetsgränserna. Verksamhetsrelaterade risker behandlas närmare i riskhanteringshandboken.

5.4 Förändringsrisker

Förändringsrisker är, som namnet antyder, risker som är förknippade med olika typer av förändringar. Riskerna kan vara interna eller bero på faktorer utanför organisationen som organisationen själv inte kan påverka. Sådana förändringar kan exempelvis rör ekonomi, lagstiftning eller lokala och globala kriser och katastrofer som tillfälligt eller permanent påverkar verksamhetsmiljön. Förändringsrisker kartläggs även när man förändrar processer inom verksamheten, även om förändringen initialt syftar till att minska riskerna. Den här processen beskrivs och preciseras närmare i handboken för riskhantering.

6. Kommunikation och rapportering

6.1 Betydelsen av och riktigheten i kommunikationen

Information och kommunikation som rör och stödjer den interna kontrollen och riskhanteringen behövs på alla nivåer i organisationen för att verksamheten ska kunna ledas i enlighet med de mål som fastställts för organisationen. För styrning och övervakning av verksamheten behöver ledningen information om mål, ekonomi, verksamhet, projekt, upphandlingar samt om gällande bestämmelser och beslut och hur dessa följs. Information om verksamhetsmiljön är också nödvändig. Denna information erhålls bland annat från parter som är kopplade till ägande, avtal, assistans eller annat samarbete.

En fungerande kommunikation som stödjer den interna kontrollen och riskhanteringen förutsätter att mål för kommunikationen fastställs och följs upp, samt att tydliga roller, befogenheter och uppgifter definieras för produktion och distribution av informationen. Dessutom behövs rutiner för hur information om den interna kontrollen och riskhanteringen ska distribueras i alla riktningar inom organisationen.

Kommunikationen med organisationens externa intressenter – såsom kunder/ kommuninvånare, serviceproducenter, revisorer, tillsynsmyndigheter och övrig statsförvaltning – måste också fungera effektivt. Från dessa externa aktörer erhålls information om brister och olämpligheter i den interna kontrollen, men även om risker som har realiserats.

För att verksamheten ska vara resultatrik måste man ha tillgång till adekvata och tillräckliga uppgifter som utgör grund för och stödjer verkställandet av den interna kontrollen och riskhanteringen. Uppgifternas riktighet, tillgänglighet och förtrolighet skyddas genom hanteringen av datarisker. Hanteringen av dessa risker omfattar metoder och rutiner som rör handläggare av uppgifter, tekniska skyddsmekanismer samt skydd av utrymmen där uppgifter hanteras.

Ansvar för ordnandet av hanteringen av datarisker och tillsynen av skyddsmekanismerna åligger den som äger informationen samt den som äger de datasystem som används för att hantera informationen. De uppgifter som hanteras måste identifieras och klassificeras för att förebygga att viktig information förändras, hanteras otillbörligt, försvinner eller blottläggs. Information i olika former (t.ex. elektroniska uppgifter eller pappershandlingar) kräver olika skyddsmekanismer.

- Hanteringen av datarisker genomförs bland annat med följande verktyg:
- direktiv, utbildning, kommunikation, utvärdering och granskningar
- klara beskrivningar av vem som äger uppgifterna och vem som innehar
- övervakningsansvaret
- klassificering och skydd av uppgifter
- tekniska datasäkerhetsrelaterade skyddsmekanismer
- hantering av tillgång till datasystem
- dokumentation av viktiga funktioner och datasystem
- bakgrundsutredningar av anställda och sekretessavtal
- uppföljning och utredning av fel och överraskande händelser
- skydd och passerkontroll som hänför sig till lokaler
- beredskap för störningar och olyckor

Det finns ingen orsak att hemlighålla uppgifter utan grund. Genom informationstransparens främjas tillgodogörandet av informationen samt bland annat den transparens och tillit som hänför sig till verksamheten och användningen av medel. Dessutom måste riktigheten och oföränderligheten hos offentlig information tryggas.

6.2 Rapportering

Det viktigaste verktyget för organisationens ledning är de rapporter som uppgörs om måluppfyllelsen och hörsammandet av stadgor och beslut samt uppdagade avvikelser. De uppgifter som rapporteras ska vara tillförlitliga, väsentliga, aktuella och i rätt form.

Kvaliteten på informationen påverkas av dess relevans, tidsenlighet, riktighet och tillgänglighet. En av de viktiga uppgifterna som utförs inom ramen för kontrollen är att se till att informationen är riktig och till sin form adekvat.

Riktigheten av informationen bekräftas med kontroll av de processer som används för att ta fram information och rapporter. Ansvaret för att riktigheten av informationen bekräftas, även av information som fåtts av externa aktörer, ligger hos den som äger ifrågavarande funktion eller process. Dessutom bör man i kontrollen av riktigheten av rapporteringen och informationen även uppmärksamma risken för oegentligheter.

Arbetet med att ta fram information och rapporter som stöder den interna kontrollen och riskhanteringen förutsätter:

- att man fastställer hurdana uppgifter som behövs
- att man identifierar informationskällor och system som producerar information
- att man kommer överens om hur informationen ska förädlas
- att man har informationsinsamlings- och distributionskanaler samt kanaler för att förmedla information
- att man har uppföljningssystem med fastställda mål, mätare och processer
- att man utreder avvikelser och tillser vidtagna korrigerande åtgärder samt
- att information och informationskällor stundom omvärderas

Det lönar sig inte att producera information ifall kostnaderna och arbetsmängden överskrider det erhållna utbytet. Information kan i allmänhet tas fram effektiverare och lättare via datasystem när informationsbehoven har tagits i beaktande redan i de krav som ställs i samband med nya datasystemsprojekt. Därför måste den interna kontrollens och riskhanteringens informationsbehov tas med i definitionen av de krav som ställs i samband med nya datassystemsprojekt.

Rapporter som produceras inom ramen för verksamhetsområdenas och resultatområdenas operativa verksamhet stöder deras egna interna kontroll och riskhantering. Enheter på olika nivåer kan i den interna kontrollen och riskhanteringen tillgodogöra sig av rapporter om bland annat:

- uppföljningen av ekonomin och verksamheten
- uppföljningen av befogenheter och användningen av dem

- avvikelser och fel
- skador och tillbud

7. Uppföljning, utvärdering och utveckling av intern kontroll och riskhantering

7.1 Uppföljning, utvärdering och utveckling på olika nivåer i organisationen

Funktionsdugligheten hos den interna kontrollen och riskhanteringen följs upp, utvärderas och utvecklas på alla nivåer i organisationen. Ansvaret för uppföljningen ligger hos de ledande tjänsteinnehavarna samt hos dottersammanslutningars verkställande direktörer och organ. I utvärderingen och utvecklingen av den interna kontroll och riskhantering som genomförs på organisationsnivå tillgodogör man sig av beskrivningar, utvärderingar och rapporterade utvecklingsåtgärder som verksamhetsområden och resultatområden har upprättat om den interna kontrollen och riskhanteringen.

Uppföljning och utvärdering utgör en viktig del av den interna kontrollen och riskhanteringen. Genom uppföljningen och utvärderingen bekräftar man funktionsdugligheten hos den interna kontrollen och riskhanteringen samt identifierar avvikelser som observerats i verksamheten och verksamhetsresultaten. Avvikelser kan vara ett tecken på en bristfällig övervakning, varvid man får en möjlighet att söka primärorsaken till bristen och vidta korrigerande åtgärder.

Verksamhetsmiljön, målen, organisationsstrukturen och verksamhetsprocesserna ändras under tidens gång. Även övervakningen måste förändras i takt med förändringarna. Genom uppföljning och utvärdering kan man bland annat:

- bekräfta att övervakningen är effektiv och funktionsduglig
- observera förändringar i verksamhetsmiljön, organisationen och verksamheten, vilka kan leda till att risker uppstår eller förändras
- lära sig av tillbud och misslyckanden
- identifiera och utvärdera avvikelser och nya risker
- utveckla den interna kontrollen och riskhanteringen

Ledningen och förmännen följer upp, utvärderar och utvecklar den interna kontrollen och riskhanteringen inom sina respektive ansvarsområden. De ska i den dagliga verksamheten följa upp risker och bedöma funktionsdugligheten och ändamålsenligheten av den interna kontrollen och riskhanteringen. Genom att förena

den uppföljningsinformation som skapas med hjälp av datatekniken med den resultatgenomgång som utförs av personalen kan man få till stånd en effektiv och ständig utvärdering. Utöver den ständiga uppföljningen som inbakats i den dagliga verksamheten och processerna måste man även genomföra periodvisa utvärderingar.

De observationer som fås via uppföljningen och utvärderingen av bristerna i den interna kontrollen och riskhanteringen ska rapporteras till de personer som ansvarar för att korrigerade åtgärder blir vidtagna. Därtill ska de observerade bristerna rapporteras i organisationslinjen till en nivå som befinner sig åtminstone en nivå högre än de personer som ansvarar för de korrigerande åtgärderna.

7.2 Redogörelse för intern kontroll och riskhantering

Bokföringsnämndens sektion för välfärdsområden och kommuner har tagit fram en allmän anvisning för upprättande av bokslut och verksamhetsberättelse. Enligt anvisningen ska styrelsen lämna en grundad redogörelse som främjar god förvaltningssed gällande den interna kontrollen i organisationen samt särskilt redogöra för koncernövervakningens tillbörlighet och tillräcklighet.

Styrelsen ska i verksamhetsberättelsen sammanställa en redogörelse för hur den interna kontrollen och riskhanteringen är ordnad, vilka brister som har identifierats i kontrollen samt hur dessa ska åtgärdas.

I redogörelsen för den interna kontrollen och riskhanteringen ska lednings- och förvaltningsseden, nuläget och utvecklingsbehoven utvärderas. Utvärderingen ska vara systematisk och tillräckligt omfattande i förhållande till organisationens storlek och struktur. Vid upprättandet av redogörelsen ska samtliga delområden som omfattas av den interna kontrollen och riskhanteringen bedömas på ett systematiskt sätt.

7.3 Användning av internrevision

Enligt välfärdsområdeslagen § 51 ska styrelsen ordna en oberoende internrevision av välfärdsområdet. Den interna revisionen är en opartisk stödfunktion för styrelsen och den högsta ledningen. Denna objektiva utvärderings-, kontroll- och konsulteringsverksamhet stöder utvecklingen av organisationen samt måluppfyllelsen. Den interna revisionen är inriktad på hela organisationens interna kontroll, riskhantering samt lednings- och förvaltningsprocesser. Den interna revisionen styrs av internationella anvisningar i branschen, vilka omfattar bland annat etiska regler, yrkesstandarder och praktiska anvisningar.

Organisationens ledning kan använda sig av intern revision för att omsätta den interna kontrollen i praktiken när den ska bedöma ledningens och förvaltningens, den interna

kontrollens och riskhanteringens resultat och tillräcklighet. Organisationen har en egen internrevisor, men organisationens ledning kan vid behov köpa denna tjänst även av en utomstående aktör. Organisationens ledning ska överväga behovet av separata utvärderingar på basis av:

- resultaten av tidigare uppföljningar och utvärderingar
- antalet förändringar som påverkar övervakningsbehovet
- naturen och omfattningen av förändringarna och de risker som är förknippade med dem
- kompetensen och erfarenheten hos de personer som sköter övervakningen

7.5 SHQS-kvalitetsprogrammet

Organisationen har förbundit sig att följa de standarder som ingår i SHQS-kvalitetsprogrammet. Självvärderingar samt både interna och externa kvalitetsauditeringar som hänför sig till kvalitetsprogrammet stöder också organisationens kontinuerliga utveckling. Genom kvalitetsledningsprocesserna utvärderas hur de interna verksamhetsmodellerna verkställs i hela organisationen. Detta bidrar i sin tur även till att den interna kontrollen fungerar ändamålsenligt.

7.6. Egenkontroll

Egenkontroll regleras separat i tillsynslagen. Organisationen ska ha ett uppdaterat egenkontrollprogram där metoderna fastställs för hur välfärdsområdet övervakar sin egen verksamhet. Med egenkontroll avses de medel och åtgärder genom vilka serviceanordnaren och serviceproducenten övervakar, följer upp och utvärderar sin verksamhet. Genom egenkontrollen säkerställs kundernas likabehandling samt tjänsternas tillgänglighet, kontinuitet, säkerhet och kvalitet.
Därtill ska välfärdsområdet tre gånger per år rapportera sina iakttagelser och korrigerande åtgärder i enlighet med egenkontrollprogrammet. Rapporten ska vara offentligt och öppet tillgänglig på välfärdsområdets webbsidor.

Välfärdsområdet ska genom egenkontroll övervaka både de tjänster som köps in och de som produceras i egen regi. Genom tillsynen ska det säkerställas att välfärdsområdet själv fullgör sina uppgifter i enlighet med lagen och att de upphandlingsavtal som det ingått följs.

8. Den externa revisionens utvärderingsuppgift

Den externa revisionen är oavhängig från den operativa ledningen och den övriga organisationen. Den externa övervakningen sköts av en revisor, revisionsnämnd och revisionsverket.

Revisor

Fullmäktige väljer en revisionssammanslutning för granskning av förvaltningen och ekonomin. Revisorn ska granska räkenskapsperiodens förvaltning, bokföring och bokslut med iakttagande av god revisionssed inom den offentliga förvaltningen. Dessutom ska revisorn granska att de uppgifter som gäller grunderna för statsandelarna är riktiga, och att organisationens interna kontroll och riskhantering samt övervakningen av ägarstyrningen har ordnats som sig bör. Revisorn avger en revisionsberättelse till fullmäktige och rapporterar om resultaten av revisionen även till organisationens ledning, revisionsnämnden och revisionsobjektet.

Revisionsnämnden

Revisionsnämndens ska bereda de ärenden som gäller granskningen av förvaltningen och ekonomin och som fullmäktige ska fatta beslut om samt bedöma huruvida de mål som fullmäktige satt upp för verksamheten och ekonomin har nåtts i organisationen. Ytterligare ska nämnden bedöma huruvida verksamheten är ordnad på ett resultatrikt och ändamålsenligt sätt. Denna verksamhet omfattar förutom organisationen och ägarstyrningen även samarbete mellan kommunerna och övrig verksamhet som grundar sig på ägande, avtal och finansiering. Nämnden övervakar att skyldigheten att redogöra för bindningar iakttas och tillkännager redogörelserna för fullmäktige. Revisionsnämnden har en egen tjänsteinnehavare, revisionschef.

Revisionsnämnden avger en utvärderingsberättelse för respektive år till fullmäktige och kan efter eget omdöme upprätta separata rapporter till fullmäktige i ärenden som är betydande för organisationens verksamhet och ekonomi.