Tel. +358 20 743 2920
www.bdo.fi

BDO Audiator Ab
Hallonnässtranden 2
FI-00210 Helsingfors

Effektivitetsrevision – Riskhanteringen vid ÅHS´ stödfunktioner och dess koppling till den interna kontrollen

Som en del av effektivitetsrevisionen av ÅHS för räkenskapsperioden 2020 har vi utfört en effektivitetsrevision av riskhanteringen och dess koppling till den interna kontrollen hos ÅHS. Fokuset i revisionen ligger på ÅHS' stödfuktioner dvs. ekonomiavdelningen, IT-avdelningen och löneavdelningen. Sjukvårdens riskhantering har inte granskats. Effektivitetsrevisionen har utförts genom att intervjua nyckelpersoner bland personalen samt genom att ta del av för revisionen relevanta dokument.

Effektivitetsrevisionen är inte en revision eller översiktlig granskning enligt ISA-standarden (International Standards on Auditing). I rapporten presenteras endast iakttagelser gällande de frågeställningar som preciseras i revisionsplanen för effektivitetsrevisionen.

Som material för effektivitetsrevision har bland annat använts:

- ÅHS' reglemente
- Diverse processbeskrivningar

Dessutom har följande personer intervjuats:

- Ekonomichefen, redovisningschefen, controllern
- It-chefen
- Personalchefen och löneredovisningsansvariga

Allmänt om intern kontroll

Allmänt kan intern kontroll beskrivas som alla arbetsrutiner och förfaranden i organisationen där samtliga förmän och redovisningsskyldiga ska garantera att verksamheten inom organisationen är effektiv, ekonomisk och lagenlig, att beslutsfattare får tillräckligt med information samt att informationen är tillförlitlig. Därtill skall en tillräcklig intern kontroll också garantera att resurser samt egendom tryggas och att organisationen följer lagar, föreskrifter och övriga beslut som har fattats inom de olika organen.

En effektiv intern kontroll bygger på en genomtänkt kontrollstruktur och ändamålsenliga kontrollåtgärder. Kontrollåtgärderna omfattar principer och verksamhetsmodeller som syftar till att hantera de risker som kan hindra att de mål som uppställts för verksamheten uppnås. Det är viktigt att kartlägga riskerna för att man ska kunna sätta in åtgärder där risker förekommer. En enskild kontrollåtgärd som vidtas mekaniskt bara för att uppfylla kravet på kontroll och utan någon tanke på vad man vill åstadkomma med åtgärden är oftast onödig.

Intern övervakning

Den interna övervakningen är en kontinuerlig övervakning av arbetsskedena eller enskilda åtgärder i anslutning till verksamheten samt medelshanteringen. Genom den interna övervakningen säkerställs att uppgifterna sköts i rätt tid såsom planerats och godkänts och inom ramen för de resurser som anvisats ändamålet. Den interna övervakningen förutsätter i allmänhet att en kontrollåtgärd skapas, vilket till exempel kan vara en viss process som säkerställer att en uppgift blir utförd på korrekt sätt. Införande av en kontrollåtgärd förbrukar alltid resurser och kan göra att en uppgift inte utförs på möjligast effektiva sätt. Kontrollåtgärder behöver trots det skapas för att säkerställa att fel eller missbruk inte förekommer. Utgångspunkten bör således vara att kontrollåtgärden fungerar som en försäkring som i slutändan leder till en inbesparing.

Den interna övervakningen förutsätter exakt definiering av befogenheter och ansvar samt täckande redovisnings- och rapporteringssystem. Alla funktioner inom en organisation behöver nödvändigtvis inte omfattas av en kontrollåtgärd. I en fungerande och välmående organisation behöver tillit ges till medarbetarna i den utsträckning som kan anses vara sund. Avsaknad av en kontrollåtgärd bör dock vara ett medvetet beslut av organisationen. Transparens minskar i allmänhet behovet av kontrollåtgärder.

Uppföljningen av ekonomin och verksamheten med hjälp av ekonomisk rapportering täcker även de områden som saknar definierade kontrollrutiner. Dessa områden faller därmed inte helt utanför övervakningen trots att definierade kontrollrutiner inte har införts.

Uppföljning

Uppföljningen är framför allt den del av den interna kontrollen som berör de förtroendevalda och de redovisningsskyldiga. Uppföljningens viktigaste uppgifter är att fastställa rapporteringsskyldighet, att kontrollera hur rapporteringen genomförs och att jämföra besluten med de resultat som beskrivs i rapporterna.

Riskhantering

Riskhantering är en väsentlig del av den interna kontrollen. Man kan säga att riskerna och hanteringen av dem är det som sätter ramarna för den interna kontrollen. Riskhanteringen kan ses som en del av organisationens strategiska, verksamhetsmässiga och ekonomiska styrning. Riskhantering är också ett verktyg som används för att säkerställa att organisationen har möjlighet att uppnå de mål som uppställts samt för att säkra att verksamheten löper oavbrutet och störningsfritt.

Riskhantering innebär att man inom organisationen identifierar risker som väsentligt inverkar på verksamheten och vidtar nödvändiga åtgärder för att säkerställa att dessa är på en acceptabel nivå. Riskerna bör identifieras, grupperas, bedömas och värderas efter rådande förutsättningar. Utgående från detta fattar man sedan beslut om hurdana kontrollåtgärder som behöver vidtas.

Risker kan hanteras genom att reducera (utfall och/eller verkningar), undvika, dela eller acceptera dem inom ramen för organisationens riskaptit. Riskhanteringen bör sträva till att uppnå rimlig säkerhet i väsentliga frågor. Fullständig säkerhet går i regel inte att uppnå utan att kostnaderna överstiger nyttan.

Till riskhanteringens skeden kan räknas bland annat måluppställning, bedömning av organisationens riskaptit (den risk som organisationen är beredd att acceptera), identifiering av risker, analys av de identifierade riskerna, bedömning och utvärdering av risker, behandling av risker, utfallsrapportering samt övervakning och uppföljning.

Beskrivning av riskhanteringen och dess koppling till den interna kontrollen inom ÅHS

Inom ÅHS' ekonomiavdelning har inte processerna och rutinerna för intern kontroll och riskhantering systematiskt och heltäckande dokumenterats. Pga. detta finns ingen tydlig länk mellan riskkartläggning och intern kontroll. På avdelningen har man arbetat en del med att dokumentera boksluts- och budgetprocessen, men de flesta andra processerna är inte dokumenterade. Avsaknad av dokumentation innebär inte automatiskt att själva arbetet är bristfälligt men gör det svårt att säkerställa hur den interna kontrollen är uppbyggd och om den är tillräcklig. ÅHS har inte alltid definierat vem som är ansvarig för olika risker. Avsaknaden av tydligt utsedda riskansvariga kan leda till lägre incitament för att identifiera och åtgärda risker och gör att ansvarsfrågor kan vara svårare att utreda om ett sådant behov uppstår.

På ekonomiavdelningen upplever man att riskmedvetenheten är rätt så hög och man försöker hantera de risker som identifierats. Arbetet med att identifiera och hantera risker är ändå inte strukturerat eller kopplat till organisationens målsättningar, utan det sker löpande och man försöker åtgärda identifierade risker efter hand.

Arbetet med identifiering och hantering av risker är inte helt strukturerat på ekonomiavdelningen. Det samma gäller för klassificering av risker. Således bedöms identifierade risker inte enligt någon bestämd skala och det kan det vara svårt att jämföra riskerna sinsemellan och bedöma vilka risker som ska prioriteras då man beslutar om vilka åtgärder som vidtas.

För upphandlings- och inköpsfunktionen finns dokumenterade kontrollfunktioner. Det finns dock inte någon dokumenterad riskkartläggning som tar i beaktande risker vid bestämmande av kontrollfunktionerna utan kontrollfunktionerna baserar sig på hittills utarbetade processer. Vi rekommenderar att en dokumenterad riskkartläggningsprocess införs som gör utarbetandet av kontrollfunktioner till ett agilt arbete, där kontrollfunktioner skapas efterhand man konstaterar att behov finns.

Inom ÅHS' löneavdelning har det inte gjorts någon systematisk riskkartläggning och processerna är inte komplett dokumenterade. I löneräkningsprocessen finns kontroller vi anser kunde förbättras. Löneräkningsprocessen innehåller många manuella skeden och användarrättigheterna är väldigt utbredda. På löneavdelningen är man ändå medveten om bristerna. För tillfället arbetar löneavdelningen med att byta lönesystem till Unit4. I samband med bytet strävar man efter att åtgärda de brister som finns. Dokumenteringen av processerna kommer att förbättras i och med bytet av system då tjänsteleverantören upprättar manualer för olika skeden i systemet.

Organisationen har arbetat med att integrera verksamhetsstyrningen med programmet Hypergene genom att föra in verksamhetsmål i programmet. Varje enhet ska sedan kvartalsvis rapportera hur målen uppnåtts. Dessa rapporter samlas in och distribueras till ledningsgruppen och styrelsen och används som verktyg i verksamhetsstyrningen. I Hypergene finns det en modul som är designad för att användas inom riskhantering. Modulen innehåller bland annat riskhanteringsmatriser som underlättar klassificeringen och bedömningen av risker. I Hypergene är det även möjligt att koppla risker till verksamhetsmål. Enligt controllern och ekonomichefen är planen att på sikt föra in risker i programmet och koppla dem till verksamhetsplaner och -mål.

På ÅHS IT-enhet sker arbetet med riskhantering dels strukturerat, dels kontinuerligt som en del av den dagliga verksamheten. I samband med projekt kartläggs och bedöms risker. Riskerna bedöms då utifrån sannolikheten för att de realiseras och konsekvenserna om de inträffar. På basis av den bedömningen vidtas åtgärder. I samband med exempelvis större uppdateringar eller systemförändringar kartläggs tekniska risker och bedöms. Även tekniska risker evalueras utifrån kriterierna sannolikhet/konsekvens och beslut om åtgärder fattas på basis av riskbedömningen.

En gång i veckan görs det inom IT-enheten en sårbarhetsskanning som körs mot en utomstående databas över kända risker. Varje vecka går man igenom de nya sårbarheterna som uppdagats och bedömer vilka som är mer akuta att åtgärda. De sårbarheter som bedöms att inte behöva åtgärdas direkt förs till en backlog och löses i ett senare skede. Även i samband med förändringar i personuppgiftshantering bedöms risker. Sådana risker kartläggs och bedöms månatligen. Däremot görs inga systematiska riskkartläggningar som omfattar hela IT-enheten.

Inom IT-enheten finns det inget skilt direktiv för riskkartläggning, riskhantering och intern kontroll. Enligt It-chefen är en del av processerna dokumenterade, men inte alla. Dokumentationen har blivit bättre och inom avdelningen arbetar man med att förbättra dokumentationen ytterligare.

Fördelar med en väldokumenterad och fungerande rutin för riskhantering och intern kontroll

Väldokumenterade och fungerande processer gör det lättare för ledningen att implementera förändringar så att organisationens arbete är i linje med de fastställda strategierna och uppställda målen. Väldokumenterade och fungerande processer bör göra det lättare för ledningen att få grepp om hur processerna och arbetssättet ser ut och därmed även vilka förändringar som bör göras. Dokumenterade rutiner gör det även lättare att identifiera och åtgärda brister i olika processer. Således torde väldokumenterade och fungerande rutiner även främja organisationens interna lärande och förståelse för riskhantering och intern kontroll.

En fördel med väldokumenterade och fungerande rutiner för riskhantering och intern kontroll är att personberoendet minskar. I en organisation utan nedtecknade processer och rutiner är personberoendet avsevärt högre. Detta beror på att nödvändig kunskap kan gå förlorad om en person som sitter på viktig kunskap inom ett visst område eller exempelvis är den enda som vet hur en specifik process ser ut samt vilka risker som är kopplade till den, lämnar organisationen.

Väldokumenterade processer gör även organisationen mer rörlig eller flexibel då det främjar förflyttning av personer inom organisationen. Det torde även vara lättare att strukturera om gällande processer och arbetssätt om alla arbetar enligt samma riktlinjer sedan tidigare. Man kan även säkerställa att nivån på arbetet som görs håller en viss nivå om alla arbetar utifrån uttänkta och fastställda processer. Dessutom leder väldokumenterade processer och tydliga ansvarsområden till att anställda är medvetna om vad de är ansvariga för samt vad som förväntas av dem. Detta medför troligen att de är mer bekväma med sina arbetsuppgifter och presterar bättre.

Omvärlden och miljöerna organisationen verkar i är sällan eller aldrig statiska, utan utvecklas och förändras hela tiden. Således är det viktigt att organisationen inte heller är statisk, utan att den utvecklas och förändras kontinuerligt. För att detta ska vara möjligt är det viktigt att processerna är agila och dynamiska. Med andra ord kan man inte se de olika processerna som stillastående och oföränderliga, utan man bör kontinuerligt utvärdera dem och bedöma om det finns behov för modifieringar. Utvärdering, men troligen också modifiering, av befintliga processer är lättare om processerna är dokumenterade.

I en organisation är det inte ändamålsenligt eller ens möjligt att helt eliminera alla risker. Vissa risker är man helt enkelt tvungen att acceptera. Det är ändå viktigt att man är medveten om vilka risker som finns. Med andra ord bör det vara ett medvetet val att inte åtgärda risker. Valet att åtgärda eller acceptera risker är en balansgång där kostnaden ställs mot nyttan av att eliminera eller minimera risken. I organisationer med bristfällig riskhantering är sannolikheten större att man drabbas av oväntade risker. Konsekvensen av att risker realiseras är antagligen mindre om man kunnat förbereda sig på möjligheten att risken realiseras. Det är således i organisationens intresse att ha en fungerande riskkartläggning och -hantering. Med hjälp av en fungerande riskhantering kan en organisation tidigt identifiera och bedöma risker och implementera kontrollåtgärder för att undvika att riskerna förverkligas eller åtminstone minimera deras inverkan. Förmågan att förstå och kontrollera risker medför även att organisationen kan vara mer trygg i besluten som fattas.

En fungerande och tydlig rutin för identifiering, klassificering och bedömning av risker ger ledningen större säkerhet då de bedömer vilka åtgärder som bör vidtas för att hantera riskerna. Detta då det på ett tillförlitligt sätt går att jämföra riskerna sinsemellan. Som tidigare nämnts är det vanligt att bedöma identifierade risker utgående från sannolikhet och konsekvens. Det vill säga hur stor sannolikheten är att risken realiseras och vilka konsekvenserna det i så fall medför. Dessa två kriterier poängsätts sedan för att utvärdera hur allvarlig risken är. Nedan är ett exempel på en riskmatris. Matrisen är tagen ur Social- och hälsovårdsministeriets publikation ”Riskhantering och säkerhetsplanering – Handbok för ledning och säkerhetsexperter inom social- och hälsovården” och torde således fungera bra inom sjukvårdsorganisationer.

Förekomsten av risk (fara, problem, oönskad händelse)					
E. Händelsen är sannolik eller ofta återkommande, kontrollen behöver förbättras i mycket stor omfattning	3	3	4	5	5
D. Händelsen är sannolik (förekommer ibland, då och då), kontrollen behöver förbättras, problem förekommer	2	3	4	4	5
C. Händelsen är möjlig, kontrollen av omständigheten behöver förbättras i viss utsträckning, problem har förekommit	1	3	3	4	4
B. Händelsen är osannolik, omständigheten är tillräckligt under kontroll, problem förekommer i ytterst liten omfattning eller inte alls	0	1	2	2	2
A. Händelsen är ytterst osannolik, omständigheten är under kontroll, inga problem förekommer	0	0	1	2	2
Konsekvenser för människor, egendom, information eller rykte	**I. Obetydliga konsekvenser**	**II. Lindriga konsekvenser**	**III. Betydande konsekvenser**	**IV. Allvarliga konsekvenser**	**V. Mycket allvarliga konsekvenser**

Figur 1: Riskmatris för bedömning av riskstorleken. (Social- och hälsovårdsministeriet, 2011)

Centrala iakttagelser och åtgärdsrekommendationer med anledning av effektivitetsrevisionen

ÅHS har inte heltäckande dokumenterade och strukturerade processer för riskhantering och intern kontroll gällande stödfunktioner. Den interna kontrollen ska bygga på och sträva efter att åtgärda de risker som identifierats i organisationens riskkartläggning. I ÅHS finns ingen tydlig länk mellan riskkartläggning, riskhantering och intern kontroll. Vi rekommenderar att man inom organisationen skapar ett ramverk eller matris för klassificering och bedömning av risker och att man med matrisen som bas gör strukturerade riskkartläggningar för att identifiera vilka risker som finns. På basis av riskkartläggningarna bör man besluta hur och vilka risker som ska åtgärdas samt vilka risker som kan accepteras.

Vi rekommenderar att man mer heltäckande kartlägger och dokumenterar processerna inom den interna kontrollen och uppdaterar processerna så att kontrollåtgärderna täcker de identifierade riskerna.

Förutom att göra organisationen mer flexibel, leder väldokumenterade processer även till ett minskat personberoende. Vi anser också att det vore bra om man i organisationen upprättar allmänna direktiv eller policys gällande riskhantering och intern kontroll samt arbetar för att säkerställa att dessa efterföljs i praktiken. Vi anser också att ledningen ta ställning till hur rapporteringen av riskhantering och intern kontroll ska ske inom organisationen. På sikt rekommenderar vi dessutom att man kopplar de identifierade riskerna till verksamhetsmål. Tanken med detta är att riskerna ställs i relation till målen, vilket torde öka sannolikheten för att de fastställda målen uppnås.

Ingen organisation är identisk en annan. Det samma gäller för riskerna organisationen hanterar. Det finns med andra ord ingen universal modell för riskhantering och intern kontroll som kan implementeras som sådan på alla organisationer. Varje organisation bör med andra ord införa och applicera en egen modell. En viktig del av detta är att fastställa organisationens riskaptit, det vill säga hur stora risker man kan acceptera i organisationen. Vi rekommenderar därför att man inom ÅHS diskuterar och utvärderar hurdana risker man är villig att acceptera och vilka man vill eliminera eller åtminstone minimera.

ÅHS är en stor organisation i vilken det rör sig stora summor pengar dagligen. Organisationen är dessutom offentlig vilket innebär att hanteringen av penningflöden bör vara särskilt varsam och transparent. Ett exempel på riskkartläggning kan vara att identifiera de mest betydande kassaflödena i organisationen samt vilka kassaflöden som av sin karaktär är extra riskabla. Utgående från denna klassificering kan ÅHS sedan ta ställning till vilka processer som ligger bakom de olika kassaflödena samt hur dessa processer bör utformas så att riskhanteringen är på en för organisationen tillfredsställande nivå.

I effektivitetsrevisionen framkom att riskansvariga inte alltid är utsedda. Vi rekommenderar således att ÅHS arbetar med att identifiera riskansvariga inom hela organisationen och därmed främja arbetet med riskhantering.

På IT-enheten inom ÅHS görs både strukturerad och mindre strukturerad riskkartläggning och -hantering. Arbetet sker både i samband med återkommande möten och löpande. De identifierade riskerna bedöms enligt sannolikhet/konsekvens och på basis av bedömningen vidtas åtgärder eller skapas kontrollfunktioner för att eliminera eller åtminstone minimera riskerna. Vi bedömer att arbetet med riskhantering och intern kontroll fungerar till väsentliga delar ändamålsenligt inom ÅHS' IT-enhet. Vi noterar ändå att dokumentationen i vissa fall är något bristfällig och rekommenderar att man strävar efter att förbättra dokumentationen för att minska risken för att fel sker samt för att minimera personberoendet inom enheten.

På ÅHS' löneavdelning har det inte gjorts någon egentlig riskkartläggning. En stor del av processerna är odokumenterade. I löneräkningsprocessen har det identifierats en del svagheter. Vi rekommenderar att man försöker åtgärda de identifierade svagheterna i samband med bytet av lönesystem, då det är ett bra tillfälle att göra förändringar i lönerutinerna. Det vore även fördelaktigt om man efter systembytet satsar på att dokumentera de interna processerna. Riskkartläggningar är ett viktigt verktyg i den interna kontrollen och rekommenderar att man i framtiden använder sig av strukturerade riskkartläggningar inom löneadministrationen.

Arbetet med riskhantering och intern kontroll är en kontinuerlig process som aldrig tar slut. Man kan med andra ord inte sätta sig ned och gå genom processerna för riskhantering och intern kontroll och sedan aldrig fundera på det igen. Organisationen och miljön organisationen verkar i lever konstant och därmed förändras även riskerna hela tiden. Således bör processerna och kontrollåtgärderna vara agila och utvecklas i takt med riskerna. Man kan således konstatera att arbetet med kartläggning och bedömning av risker bör ske kontinuerligt så att organisationen ständigt kan vidta effektiva åtgärder för att hantera riskerna den ställs inför.

Mariehamn den 20 januari 2021

BDO Audiator Ab, revisionssammanslutning

Andreas Holmgård
OFGR, CGR