Jämtlands Läns Landsting

Missiv

Landstingets revisorer

Tf Revisionsdirektör Majvor Enström
Tfn: 063- 147528

2009-12-15

Dnr REV/18/2009

Landstingsstyrelsen

Landstingets löneadministration – Granskning av interna kontrollen

Revisionskontoret har på vårt uppdrag och med hjälp av Ernst & Young granskat landstingets löneadministrativa rutiner. Det övergripande kontrollmålet i granskningen har varit att ge svar på om den interna kontrollen är tillfredsställande och ge besked om det finns brister i den interna kontrollen inom löneadministrationen som bland annat skulle kunna innebära risk för förskingring.

Resultatet av granskningen redovisas i bifogad granskningsrapport.

Inledningsvis vill vi uppmärksamma på att några åtgärder redan har vidtagits av de ansvariga för löneadministrationen som i en positiv anda hörsammat våra rekommendationer.

De viktigaste iakttagelserna och synpunkterna är följande:

- Rutiner och organisation för administrering av behörigheter till det löneadministrativa systemet Heroma bör förbättras. Det är inte tillfredsställande att tilldelning av behörigheter sker utan en skriftlig ansökan och beslut från överordnad. En förbättringsåtgärd är att utarbeta ansökningsblankett för nämnda ansökan. Vi rekommenderar även att det görs systematiska genomgångar av gällande behörigheter och att det tas fram en dokumentation över vilka som har behörigheter till det löneadministrativa systemet och behörigheternas omfattning. Dokumentationen bör även omfatta rutiner för ändring och borttagande av behörigheter, för att säkerställa att behörigheterna är väl anpassade till användarens arbetsuppgifter.

- Kontrollen i lönerutinen bör förstärkas för att minska risken för felaktiga löneutbetalningar. Vi rekommenderar bland annat skärpt kontroll av löner till personal med höga behörigheter samt att rutinen för upplägg av nyanställda sker enligt ”tvåhandsprincipen”.

- Säkerheten kring externa leverantörens (Logica) åtkomst till landstingets lönesystem mm måste skärpas eftersom dessa användare har oinskränkta behörigheter. Detta i kombination med att gruppbehörigheter används och att identifikation endast görs med hjälp av lösenord gör att vi bedömer det nödvändigt att förbättra säkerheten på dessa områden.

Vi föreslår även att det införs ett allmänt krav på att leverantörer skall använda någon form av förstärkt identifieringskontroll. Landstingets interna regler om att eID (smarta kort) ska användas för användarautenticiering bör även omfatta externa leverantörers inloggning till landstingets nätverk/domän.

- Åtgärder bör snarast vidtas för att skydda loggarna. Syftet med loggar är att i efterhand kunna följa upp och kontrollera bland annat vad som registrerats, av vem samt när registreringen utfördes. Nuvarande hantering av loggarna medför risk för att nödvändiga uppgifter, för felsökning och för utredning vid misstänkt bedrägeri, raderas. Denna risk måste snarast undanröjas.

- Det uppstår differenser mellan vissa konton i lönesystemet Heroma och ekonomisystemet Raindance Skillnaden har bestått i att främst semesterlöneskulden i Heroma varit lägre än motsvarande skuld i Raindance. Differenserna har enligt uppgift inte heller varit möjlig att helt reda ut. Det bör vidtas åtgärder för att komma till rätta med nämnda differenser och därmed minska risken för att felaktiga transaktioner från lönesystemet kan undgår upptäkt.

Vi emotser senast den 1 april 2010 en redovisning av vilka åtgärder som landstingsstyrelsen vidtar eller avser vidta med anledning av granskningsresultatet.

För Jämtlands läns landstings revisorer

Mona Nyberg
Ordförande

Jöns Broström
V ordförande

Bilaga
Rapporten Granskning av landstingets löneadministration.

Kopia till
Fullmäktiges presidium
Landstingsdirektören
Bitr. landstingsdirektören
Chefen för ledningsstab IT
Chefen för ledningsstab personal

REVISIONSRAPPORT
Granskning av landstingets löneadministration

Ansvarig: Jonas Wiberg

Revisor

INNEHÅLLSFÖRTECKNING

1 SAMMANFATTNING

Det övergripande kontrollmålet med denna granskning är att ge svar på om den interna kontrollen är tillräcklig inom löneadministrationen och ge besked om det finns brister i den interna kontrollen inom löneadministrationen som bland annat skulle kunna innebära risk för förskingring.

I vår granskning har vi uppmärksammat följande brister.

- Systemhandläggare skulle ha kunnat manipulera sin egen lön.
- Svårigheter i att stämma av jourskuld och semesterskuld.
- Brister i uppföljning av behörighetstilldelning.
- Loggar går att radera
- Det saknas en aktuell och tydlig beskrivning av lönerutinen
- Upplägg av nya personer sker inte via tvåhandsprincipen

För att en ottillåten utbetalning ska kunna äga rum utan att det upptäcks krävs att några kriterier är uppfyllda. Möjlighet att manipulera sin egen lön, alternativt att det går att lägga upp en medbrottsling i systemet utan att någon reagerar. För att utbetalningen inte ska upptäckas krävs även konton och kostnadsställen där denna transaktion kan konteras utan större risk för upptäckt. Eftersom dessa kriterier initialt var uppfyllda anser vi att det i teorin gick, för några få individer, att göra otillåtna utbetalningar men att risken för upptäckt ändå var relativt hög.

På vår rekommendation, i samband med intervjuer, har lönekontoret nu, enligt uppgift ändrat en rad rutiner och behörighetstilldelningen. Dessa ändringar är inte testade av oss men vi har i våra slutsatser samt rekommendationer utgått från att lönekontorets åtgärder är utförda på rekommenderat sätt.

Vår bedömning är att landstinget genom ytterligare några insatser kan stärka den interna kontrollen.

De viktigaste förbättringsområdena är:

- Det bör inte finnas konton där felaktiga transaktioner kan undgå upptäckt. Differenser som uppstår vad gäller jour-, övertid och semesterskuldskontona måste utredas.
- Upplägg av nya personer bör göras av två personer alt attesteras av någon överordnad.
- Möjligheten att radera loggar måste spärras
- Ökade kontroller av utbetalda löner till personer med hög behörighet. Undersöka om webbtjänst för kontroll av lönespecifikation går att använda
- Inför stärkt identitetskontroll för inloggning till landstingets servrar för externa leverantörer
- Ställ krav på att externa leverantörer kan styrka att de har en tillräcklig säkerhet innan de ges behörighet att logga in på landstingets servrar

2 INLEDNING/BAKGRUND

Jämtlands läns landsting (JLL) betalade under år 2008 ut lön till totalt ca 4 500 personer, de flesta månatligen. Under ett år betalar lönekontoret ut ca 900 miljoner kronor i nettolöner. Detta gör att lönekostnaderna är en av jämtlands läns landsting i särklass största utgiftsposter och att lönekontoret är den avdelning som hanterar de största utbetalningarna.

Landstingets revisorer har mot bakgrund av sin risk- och väsentlighetsanalys bedömt det angeläget att genomföra en granskning av jämtlands läns landsting löneadministrativa rutiner. Granskningen avses ge besked om det finns brister i den interna kontrollen inom löneadministrationen och som bland annat skulle kunna ge upphov till förskingring av medel.

3 SYFTE, REVISIONSFRÅGA OCH AVGRÄNSNING

Det övergripande kontrollmålet är att ge svar på om den interna kontrollen är tillräcklig inom löneadministrationen.

Granskningen är avgränsad till de rutiner och system som hanteras centralt av lönekontoret inom ledningsstab personal samt rutiner inom ledningsstab ekonomi vad avser bokföring och avstämning av löneutbetalningar.

4 REVISIONSKRITERIER

Revisionskriterierna utgår från:

Begreppet god intern kontroll

Ett bra system för intern kontroll ska minska risken för att fel i det dagliga arbetet, såväl avsiktliga som oavsiktliga, leder till fel i redovisningen. Den interna kontrollen kan dock inte fånga upp alla fel och dessutom kostar intern kontroll pengar. Kostnaden för kontrollen måste alltid vägas mot den fördel i form av minskad risk som den kan ge. Till intern kontroll hör att ansvars- och arbetsfördelningen är genomtänkt och fungerar. Attest- och rapportsystemen måste vara ändamålsenliga. En bra ansvars- och arbetsfördelning innebär bl.a. att ingen person ensam ska kunna hantera en transaktion i alla led. Utifrån detta har vi satt upp ett antal revisionsfrågor som vi sökt svar på och vars svar sedan ligger till grund för bedömningen om den interna kontrollen är tillräcklig inom löneadministrationen. Revisionsfrågorna behandlas under resultat.

5 GRANSKNINGSANSVARIG

Ansvarig projektledare har varit Ulf Rubensson., certifierad kommunal revisor vid landstingets revisionskontor.

Granskningen har, under ledning av landstingets revisionskontor, utförts av Jonas Wiberg vid Ernst & Young AB.

6 METOD

Granskningen har genomförts främst genom intervjuer med nyckelpersoner inom löneadministrationen samt även systemhandläggare och personal på ekonomiavdelningen med kopplingar till lönesystemet. Vi har i möjligaste mån även testat de kontroller som lönekontoret säger sig ha. Detta gäller t.ex. allt från avstämningar till automatiska kontroller/spärrar i lönesystemet.

Granskningen har haft ansatsen att analysera om befintliga kontroller är ändamålsenliga och att lämna förbättringsförslag.

7 RESULTAT

7.1 SYSTEM & ROLLER

Löneprocessen är en invecklad rutin. Det finns en rad olika roller som är involverade i kedjan från upplägg av nyanställning till en faktisk löneutbetalning. För att klargöra rollerna lämnas under avsnitt 7.1.2 nedan en förenklad beskrivning. Vår granskning av den internkontroll utgår huvudsakligen från vad dessa olika grupper kan göra. Det förekommer även en del systembegrepp som kan var svåra att förstå och som vi därför, inledningsvis, försöker förklara.

7.1.1 System

Lönesystemet heter Heroma och det är ett personal- och löneadministrativt system som utvecklas av Logica och det används av en rad andra landsting. Logica är ett multinationellt telekom- och IT-företag som år 2006 köpte svenska IT konsulten WM-data. Systemet innehåller olika delsystem, de vi kommer att beröra är behörighetsmodulen Berit och styrregistret.

I Berit läggs behörigheterna upp, det är bland annat här som det går att styra om användaren ska spärras så att denne inte kan göra förändringar av de egna uppgifterna i lönesystemet. Vidare finns ett styrregister där kopplingar mellan lönearter och kostnadsställen läggs upp.

Enkelt utryck kan sägas att lönesystemet i grund och botten är en databas bestående av en mängd tabeller med information om anställda, löner, kopplingar till konton mm. Att arbeta direkt i databasen kräver kunskap i bland annat programspråket SQL. Det är via SQL som allt utförs och hämtas.

För att bl. a underlätta handhavandet av de kommandon som kan ges med SQL finns QM (Query Manager). Det är ett program som också arbetar direkt med SQL databasen. Idag används programmet bara för att få fram data ur databasen. Det är bara en person som överhuvudtaget använder programmet, dock är det de båda systemadministratörerna och systemansvarig som har tillgång till det.

Detta är inte någon användarvänlig miljö och därför finns en applikation som gör gränssnittet ut mot användaren bättre och mer lättarbetat. Det är denna applikation som är Heroma.

Många av de befintliga kontrollerna och loggmöjligheterna är inbyggda i applikationen Heroma. Det som är problemet, ur ett internkontrollperspektiv, är att den som arbetar direkt med SQL eller QM mot databasen oftast undgår kontrollerna. Vilka kontroller som finns i QM, eller hur den loggas, vet inte löneavdelningen.

7.1.2 Roller

Personalhandläggaren
Arbetar inte med löner utan enbart med att registrera anställningar i Heroma. De registrerar person-uppgifter, anställningsuppgifter och skriver ut anställningsavtal. Dessa personer finns ute i respektive verksamhet. De har ingen behörighet att ändra eller justera lönerna.

Löneadministratörer
Arbetar på lönekontoret. De kan utföra personalhandläggarens arbete men gör det sällan. Deras främsta syssla är lönebearbetning. De justerar avvikelser i tid och lönerapporteringen, gör ombokningar och rättningar. De utför olika kontroller på lönekörningen, stora belopp mm.
De har ingen tillgång vare sig Berit eller styrregistret.

Systemhandläggare
De finns två systemhandläggare. Deras uppgift är enkelt uttryck att se till att lönesystemet fungerar som det ska. De testa uppdateringar, lägger upp behörigheter, kopplar lönearter till kostnadsställen samt sköter de driftsfrågor som landstinget ansvar för enligt avtalet med Logica. Systemhandläggarna har tillgång till hela lönesystemet inkl Berit och Styrregistret. Båda har även tillgång till QM men bara en av dem kan med programmet.

Systemansvarig
Utgörs av en person. Denna person är den enda som har tillgång till möjligheten att stänga av möjligheten att ändra sin egen lön. I övrigt har personen bara läsbehörighet i lönesystemet och kan således inte ändra sin egen lön.

7.2 REVISIONSFRÅGOR: BEDÖMNINGAR & REKOMMENDATIONER

Som beskrivits ovan har vi satt upp ett antal revisionsfrågor som rör den interna kontrollen. Svaren på dessa är det som ligger till grund för vår bedömning om statusen på den interna kontrollen.

Vid intervjuerna och testningen av de kontroller som löneadministrationen säger sig ha har följande framkommit.

Revisionsfråga:

1. Begränsas behörighet i lönesystemet så att löneadministratörer inte kan behandla och/eller manipulera sin egen lön?

Löneadministratörerna har inte behörighet att påverka sin egen lön. Detta styrs genom behörighetstilldelningen i systemet Berit. De två som ansvarar för behörighetstilldelningen, två systemhandläggare, kunde dock ta bort denna spärr inklusive på sig själv.

Bedömning
Möjlighet att genom registreringar kunna påverka sin egen lön är ur ett internkontrollperspektiv oacceptabelt. I detta fall rörde det sig om två systemhandläggare som enligt vår granskning kunde göra detta. Anledningen till att de överhuvudtaget kunde det är att det vid upplägg av behörigheter i löneprogrammet fanns en tillvalsfunktion där systemhandläggarna kunde göra ett val så att de skulle ha kunnat påverka sin egen lön.

Vad vi kunnat se finns det ingen anledning att denna funktion måste finnas. Vi rekommenderade därför lönekontoret att kontakta programleverantören för att, om möjligt, stänga funktionen.

Åtgärder från lönekontoret med anledning av våra rekommendationer
Enligt lönekontorets utsago har de nu tagit bort systemadministratörerna behörighet till denna funktion. Numera är det endast systemansvarig som har behörighet till denna funktion. Systemansvarig har i sin tur enbart läsbehörighet till resterande del av lönesystemet. Vår bedömning är att lönekontoret därmed har vidtagit åtgärder som undanröjt den iakttagna bristen avseende möjligheten att någon på egen hand kan skapa sin egen lön. Därmed har den största iakttagna bristen åtgärdats.

Revisionsfråga:

2. Är rutiner och organisation för behörighetsadministrationen lämplig med avseende på intern kontroll?

Idag finns ingen tydlig rutin för behörighetstilldelning. Lönekontoret har alltid haft för avsikt att alla beslut om behörighetstilldelning ska komma skriftligen men så har inte alltid skett. I vissa fall har de erhållit mejl med begäran om en behörighetstilldelning. När vi önskade att se vilka som har administratörsbehörighet till Heroma gick det inte att ta fram en lista på det. Person för person var det möjligt att se vilken behörighet användaren hade men för att få fram en lista krävdes det att

informationen togs ut via QM. SQL kunskaperna var dock inte tillräckliga för att få fram listan. Lönekontoret är själva medveten om att denna rutin kan förbättras varför kontakt tagits med andra landsting för att kunna förbättra denna rutin. Ambitionen är att det numera ska gå ut en blankett till den chef som beslutat om en behörighetstilldelning. Vidare ska behörigheterna ses över. Istället för att tilldelning till olika delar av systemet sker allt efter som behoven uppstår är tanken att det ska finnas färdiga roller som innebär en viss behörighetsnivå. I samband med att rollupplägget görs är tanken att en översyn av dagens behörigheter ska gås igenom.

Bedömning
Det är inte tillfredsställande att det finns brister i behörighetstilldelningen. Alla beslut rörande behörighetstilldelning måste följa en fastslagen rutin och beslutet måste vara skriftligt. Det får vidare inte råda någon osäkerhet kring utdelade administratörsbehörigheter.

Lönekontoret tycks medveten om att det finns vissa brister i behörighetstilldelningen varför en förändring är på gång. I detta fall anser vi dock att det största problemet är att det inte finns dokumentation kring vilka som har vilka behörighet till vad, rutiner för bortplockning av behörigheter och dokumentation när någon erhållit behörigheter utöver sin rollbehörighet. Det finns exempelvis idag inget aktuellt dokument över vilka som har skrivrätt i programmet för behörighetstilldelning, vilket vi anser bör finnas.

Systemhandläggarnas behörigheter är omfattande. Att avväga rätt behörighet mot internkontroll är dock svårt. Det är ofrånkomligt att det måste finnas systemadministratörer med stora behörigheter. Dock bör man i möjligaste mån styra avstämningsarbete och kontroller så att den interna kontrollen fortfarande kan upprätthållas. Exempel på detta kan vara kontroller som gör att felaktigheter lätt upptäcks, exempelvis utökade kontroller av utbetalningar till personer med höga behörigheter.

Rekommendation

Gör systematiska genomgångar av gällande behörigheter.

Förbättra dokumentationen av behörighetstilldelningen, aktuella listor bör finnas på vilka som har behörighet att göra registreringar i bland annat Berit, styrregistret och QM. Skriftlig dokumentation ska även finnas vid beslut om behörigheter utöver sin rollbehörighet, likaså rutiner för tillfälliga behörighetstilldelning för exempelvis konsulter.

För personer med behörighet som innebär möjlighet att använda SQL-kommandon eller att använda QM rekommenderar vi att landstinget försöker hitta förstärkta kontroller (gäller bl.a. systemadministratörerna för Heroma och personal från Logica).

Vi anser att det är bra att lönekontoret har för avsikt att ta fram färdiga behörighetsroller. Inriktningen bör vara att vissa arbetsuppgifter innebär en viss roll vad gäller behörighetstilldelningen. På så sätt förenklas arbetet med tilldelningen av behörigheter samt att risken för att någon får ”för höga” behörigheter minimeras.

Ett exempel på problem vid manuell tilldelning av behörighet är när någon byter tjänst. Om nya behörigheter bara byggs på kan det i slutändan innebära att en anställd sitter på en, ur ett internkontrollperspektiv, olämplig kombination av behörigheter.

Åtgärder från lönekontoret med anledning av våra rekommendationer
Lönekontoret uppger att de har tagit till sig av vår rekommendation och att de kommer att ta fram bättre rutiner/beställningsblanketter för behörighetstilldelning.

Revisionsfråga:

3. Finns tillräckliga kontroller för onormala belopp för nettolön per anställd och onormala belopp på enskilda lönearter/ersättningar? Finns ändamålsenliga regler för handläggningen av avvikelser och följs dessa samt utförs specifika kontroller av åtgärder som utförs av systemadministratören (-er) och eventuella andra med höga behörigheter på ett tillfredsställande sätt?

I lönesystemet (Heroma) finns en rad automatiska kontroller. Exempel på detta är avvikande lön från genomsnitt, hög bruttolön, ej godkända stämplingar mm. Dessa avvikelser framgår av signallistan och de bygger på förinställda regler/gränsvärden i Heroma. Rutinen är att denna signallista månatligen granskas post för post för att se om det finns en rimlig orsak till att löneprogrammet påkallat uppmärksamhet. Någon speciell kontroll av personer med höga behörigheter finns idag inte.

Bedömning

Det är svårt att bedöma om de automatiska kontrollerna skulle fånga upp alla typer av fel. Exempelvis verkar den inte beakta tillägg utanför lönen, så som utbetalning för utlägg. Ett sätt att komma runt det skulle kunna vara att göra avvikelsekontrollen på utbetalat belopp istället för bruttobeloppet. Personalen anser även att signallistan blir lite för lång, för många träffar. Risken med det är att granskningen inte görs i tillämplig utsträckning. Vi har kontrollerat om kontrollen av signallistan sker på uppgivet sätt och bedömer att kontrollen fungerar.

Rekommendation
Vi har rekommenderat att den ansvarige på löneadministrationen går igenom förslaget till utbetalningslista (SPADAB lista) som kommer från Logica med avseende på de personer som har höga behörigheter innan klartecken lämnas till Logica. Listan är i personnummerordning vilket gör det till en relativt enkel kontroll. Det är enligt vår bedömning omöjligt att en lön betalas ut utan att det syns på denna lista varför den utgör ett bra underlag för kontroll med avseende på upptäcktsrisken. Vidare bör man se över om gränsnivåerna går att höja vad beträffar de automatiska kontrollerna samt att undersöka om avvikelse utifrån genomsnittlig utbetalning går att få fram på ovan nämnda signallista.

Vi rekommenderar även att undersöka om kopia på lönespecifikationen går att erhålla som en webbtjänst. Swedbank har exempelvis denna tjänst. Tjänsten innebär att lönekontoret via inloggning mot bankens internetsida kan se kopia på den faktiska lönespecifikationen på det personnummer som administratören söker på. Kopian går inte att ändra eftersom lönekontoret bara har läsbehörighet. Detta skulle göra kontrollen av faktiskt utbetalda löner betydligt lättare.

Åtgärder från lönekontoret med anledning av våra rekommendationer
Direkt efter att vi lämnat våra synpunkter ändrades rutinen vad gäller kontroll av utbetalningslistan.

Numera är det enligt uppgift den systemansvarige på löneadministrationen som går igenom förslaget på utbetalningslistan.

Revisionsfråga:

4. Görs tester av program-, register- och andra uppdateringar i en särskild och tillfredställande testmiljö?

Detta arbete sköts till viss del av både lönekontorets systemhandläggare och leverantören Logica. Innan Logica skickar ut en uppdatering testar de själva programmet. Därefter erhåller systemhandläggarna en testversion som sedan ska kvalitetssäkras. Om den anses korrekt görs uppdateringen i produktionsversion (den skarpa). All testning görs med samma konfiguration som programvaran sedan körs skarpt på och det är enbart systemhandläggarna som får godkänna en implementering i den skarpa miljön. Det som testas är i grund och botten att programmet uppför sig som det ska efter uppdateringen. Att det inte uppstår onormala felmeddelande och att funktionaliteten är intakt. Logica skickar ut flera typer av uppdateringsförslag. En del uppdateringar är större, programuppdateringar medan en del kan röra mindre förändringar i tabellverk. Uppdateringarna är inte tvingande, systemhandläggarna beaktar om detta behövs. I de allra flesta fall görs dock den föreslagna uppdateringen. Anledningen att inte genomföra en uppdatering kan exempelvis vara att uppdateringen är av mindre karaktär inte berör löneadministrationen vid Jämtlands läns landsting.

Det finns två testmiljöer för tester av program, en miljö som är som en kopia av den skarpa och en annan där kommande versioner läggs upp. Det är enbart lönekontoret som har tillgång till testmiljön. Dagens avtal med Logica är under omarbetning där förtydligande kring ansvar och test kommer att göras. Systemhandläggarnas ansvar kommer att minska i och med det nya avtalet.
Logicas del av driften inbegriper att de delvis står för övergripande support men även att de gör själva lönekörningen, tar hand om felanmälan samt gör nattkörningar. Vad Logica får göra och inte göra regleras i avtalet.

Felanmälan innebär att Logica begär att få en kopia på databasen, Logica gör sina tester och återkommer med anvisningar om hur systemhandläggaren ska kunna lösa problemet på egen hand.

Lönekörning innebär att Logica samlar ihop informationen i lönesystem, sammanställer det skickar en utbetalningsfil till banken.

Nattkörning innebär att Logica går in i systemet och gör uppdateringar av register och styrtabeller samt gör säkerhetskopiering. Logica har egen fast förbindelse till landstingets Heromaservrar. Logicas närvaro syns i driftsrutinen och vad de gjort syns i loggen. (*Se vidare revisionsfråga 5 nedan*).

Bedömning
Det finns tillgång till miljöer där tester kan göras innan ändringar görs i produktionsmiljön, men det är svårt att kontrollera testmiljöerna i praktiken och vi kan därför inte uttala oss om testmiljöerna som sådana är tillfredsställande.

Revisionsfråga:

5. Är de loggar som finns tillräckliga, görs tillräckliga kontroller av loggarna samt utförs kontrollen av personer med tillräcklig kunskap?

Heroma är installerad på servrar som finns hos landstinget. Landstinget har ett avtal med Logica om att svara för fjärrdriften av dessa servrar. Logica har av den anledningen en egen fast förbindelse till landstinget.

Det finns loggar på olika ”nivåer”. Dels loggas vilka som släpps in genom brandväggen, dels vad som görs i ”domänkontrollanten”[1)], dels vad som görs i systemmiljön på servrarna och dels vad som görs i applikationen Heroma. Det finns inga klara regler för vad som ska loggas och hur loggarna ska hanteras med avseende på bevarande och uppföljning. Det finns betydande problem med volymen av den mängd data som sparas i loggarna. Loggarna gallras av den anledningen ut efter en ibland mycket kort tid. Generellt kan man säga att desto längre ”in i systemet” man kommer desto längre tid finns loggarna sparade. För närvarande sparas Heromas loggar, enligt uppgift, till dess historikdatabasen töms. I nuläget finns uppgifter från år 2003.

Vid samtal med ansvarig för landstingets IT-infrastruktur samt IT-säkerhetsansvarig framkom att personalen vid Logica loggar in på Heromaservrarna med en gruppanvändaranvändaridentitet och ett lösenord. Gruppanvändaranvändaridentiteten ger full behörighet på de servrar där Heroma är installerade. Med detta följer även en möjlighet att radera loggar. Avseende det senare finns det tekniska lösningar som man tittar på och det har även gjorts några provinstallationer (dock inte på någon Heromaserver) av en produkt som ska kunna lagra loggar på sådant sätt att data inte kan raderas. Något beslut om allmänt införande av detta loggskydd finns ännu inte.

Enligt uppgift från landstingets IT-säkerhetsansvarige är landstingets policy ifråga om autenticering att gruppkonton inte ska användas. Det gäller både interna och externa användare. I vissa fall där annan lösning än gruppkonto inte skulle fungera kan dispens beviljas av systemägare IT-infrastruktur. Men något sådant fall föreligger inte med Logica. De ska använda personliga konton för inloggning.

I landstingets dokument ”Regler och Riktlinjer för teknisk IT-infrastruktur bas” Dnr: LS/1239/2005, anges att “vid inloggning till JLL:s nätverk/domän ska eID (smarta kort) användas för användarautenticering”. Enligt uppgift är detta under införande. Vid halvårsskiftet 2011 kommer ca 90% av de anställda att ha fått sitt kort (sk SITHS-kort).

Enligt uppgift brukar landstinget ha med i avtalet gentemot externa leverantörer att deras personal och ev. anlitade underleverantörer ska följa hos landstinget gällande säkerhets- och sekretessföreskrifter mm. Beträffande sekretessen brukar det anges att leverantören ska kunna visa att all personal som på något sätt utför uppdrag åt Landstinget undertecknat en sekretessförbindelse. Något krav på att leverantörerna ska kunna styrka att de upprätthåller en tillräcklig säkerhet finns dock inte med och det anges inte heller vad som är tillräcklig säkerhet.

I avtalet med Logica sägs att deras personal skall vara väl förtrogna med miljö, driftrutiner och säkerhetsregler. Det sägs också att de regler som anges under ”Säkerhet och Sekretess” i Beställarens IT-policy och IT-strategi ska gälla. I dessa dokument finns dock inget avsnitt med denna rubricering. I det senare dokumentet finns en hänvisning till att regler och anvisningar för IT-säkerhet anges i

[1)] ”domänkontrollanten”= ett behörighetsregister som bl a håller reda på vilka applikationer och andra resurser som resp användare ska ha tillgång till.

IT-säkerhetsplanen med tillhörande riktlinjer. Det dokumentet handlar dock mer om hur arbetet ska gå till för att avgöra vilket skydd som behövs.

För närvarande finns det inga tydliga regler som gäller för vilka villkor och säkerhetsarrangemang som ska vara uppfyllda innan en leverantör ”släpps in” i landstingets datamiljö (därmed inte sagt att det görs utan prövning). Ett dokument benämnt Riktlinjer för IT-säkerhet i IT-infrastrukturen är dock under framtagande och uppges vara klart inom en snar framtid.

Som nämnts inledningsvis, är många av de befintliga kontrollerna och loggmöjligheterna inbyggda i applikationen Heroma. Det som är problemet, ur ett internkontrollperspektiv, är att den som arbetar direkt med SQL eller QM mot databasen oftast undgår kontrollerna. Vilka kontroller som finns i QM, eller hur det loggas, vet inte löneavdelningen. Till bilden hör även att de två systemhandläggarna har tillgång till hela lönesystemet inkl Berit och Styrregistret. Båda har även tillgång till QM

Generellt kan sägas att en person med goda kunskaper i SQL samt med möjlighet att gå in i löne-systemet kan göra i princip vad som helst. De personer som har en sådan behörighet utgör därför en potentiell risk. Det som kan ha en preventiv effekt är skyddade loggar.

I Heroma loggas allt som rör förändring av exempelvis fast lönedata, lönesumma, adressuppgifter mm. Likaså loggas korrigeringar i löner mm. Enligt lönekontoret loggas ”i princip allt”. Behörighet till loggarna har Logica, systemhandläggarna och systemansvarig.

Någon rutinmässig kontroll av loggarna i Heroma görs inte. Loggarna används när ”något blivit fel” för att dels se vad som gjorts och dels tillrättavisa vid handhavandefel. I loggen syns vem som gjort vad och vilken tid. Det som kopplar ihop loggen med en användare ett användar-ID.

Bedömning
Det finns vissa risker med det arrangemang för åtkomst som Logica har.

- Gruppanvändaridentiteter bör inte förekomma. Det medför att det inte går att utläsa ur loggarna vilken individ det är som gjort vad. De oinskränkta behörigheterna utgör också en risk. Kombinationen är definitivt olämplig.
- Det bör kunna ställas krav på att externa leverantörer kan styrka att de har en tillräcklig säkerhet innan de ges behörighet till landstingets servrar, i vart fall när det är fråga om den högsta behörighetsnivån. Exempel på sådana krav är att personalen fått den utbildning om landstingets regler och rutiner som avtalats, att de fått den utbildning som behövs för arbetet i övrigt, att man har interna regler för vad de anställda får göra och inte och att det finns en fungerande uppföljning av efterlevnaden, samt motsvarande gäller även för ev. underleverantörer.
- Enbart lösenord är för svagt som identifikationsmetod mot bakgrund av de värden som skall skyddas och den omfattande behörighet Logicas personal tilldelats.

Enligt de test vi utfört anser vi att loggarna i Heroma är tillfredställande vad gäller dess innehåll och möjligheten till spårning av användare. Detta anser även de som använder dem. Vår bedömning är även att de som kontrollerar loggarna har den kunskap de behöver. Det är dock oacceptabelt att loggarna kan raderas. De två systemhandläggarna kan radera gamla loggar vilket både vi och de själva anser vara en allvarlig brist i kontrollsystemet. Därmed faller loggen delvis som ett verktyg vid misstänkt bedrägeri.

För att loggarna ska få en tillräckligt preventiv effekt är det viktigt att uppföljningen av dem sker aktivt utifrån en bedömning av risk och väsentlighet och att det finns en plan för kontrollerna.

Rekommendation.

Gå igenom vilket syfte och vilka intressenter de olika loggarna har och bestäm vilka kontroller som ska göras, av vem, hur ofta och arkiveringstid. Enligt vår mening bör det ske en aktiv uppföljning av loggarna på Heromaservrarna och av loggarna för applikationen Heroma, framför allt riktad mot åtgärder vidtagna av personer med höga behörigheter.

Vidta åtgärder för att skydda de loggar som innehåller bevisvärden som kan vara nödvändiga om oegentligheter skulle upptäckas. Att loggarna är skyddade från radering och förändring ger också en preventiv effekt.

Inför ett allmänt krav på att externa leverantörer skall använda någon form av förstärkt identifieringskontroll. Landstingets interna regler om att eID (smarta kort) ska användas för användarautenticiering är bra och bör även omfatta externa leverantörers inloggning till JLL:s nätverk/domän.

Jämtlands läns landsting har beslutat att BITS ska gälla som basnivån för informationssäkerheten. BITS är Krisberedskapsmyndighetens rekommendationer vad gäller basnivå för IT-säkerhet

I BITS kapitel ”6.2 Utomstående parter” finns som basnivå bl. a angivet att det ska finnas dokumenterade regler för tredjeparts åtkomst till information eller informationssystem, att extern personal ska informeras om regler för åtkomst mm. Det finns även angivet vad avtal med utomstående parter bör beakta. Dessa krav bör tas med i det kommande dokumentet ”Riktlinjer för IT-säkerhet i IT-infrastrukturen”.

Förutom att ställa krav i avtalet om säkerhet bör landstinget begära att leverantörerna kan styrka att de uppfyller kraven. Begär därför att Logica kan styrka att deras säkerhet är tillräcklig. Detta är en prövning vi anser att alltid bör göras avseende alla externa leverantörer, med långtgående behörigheter, innan de ges tillträde till landstingets servrar. Detta krav bör ingå som ett skall-krav i samband med upphandlingar.

Åtgärder från lönekontoret med anledning av våra rekommendationer

Enligt uppgift från lönekontoret avser de att försöka lösa problemet med att systemadministratörerna haft möjlighet att radera loggar i Heroma via tilldelning av behörigheter på samma sätt som beskrivits under fråga ett.

Åtgärder från ansvariga för IT-infrastruktur och IT-säkerhet

Enligt uppgift från ansvarig för IT-infrastrukturen kommer åtgärder att vidtas som gör att Logicas personal erhåller personliga användaridentiteter. Pga. av vissa programtekniska omständigheter kommer dock en gruppanvändaridentitet att finnas kvar för vissa funktioner där det för närvarande inte finns andra tekniska lösningar.

Enligt uppgift från landstingets IT-säkerhetsansvarige kommer det styrande dokument som är under framtagande (Riktlinjer för IT-säkerhet i IT-infrastrukturen) att reglera detta på en betydligt mer täckande nivå än vad som är fallet idag. I dokumentet kommer att ställas uttryckliga krav på hur anslutningen ska få ske samtidigt som man kommer att ”ta höjd” för alla BITS-krav som gäller för extern åtkomst.

Revisionsfråga:

6. Dokumenteras förändringar och uppdateringar av registeruppgifter i lönesystemet och är det säkerställt att dessa alltid attesteras/kontrolleras av annan än den som har registrerat/infört uppgifterna?

Den vanligaste typen av uppdateringar är förändring av lön. Vid den stora löneöversynen läggs alla uppgifter upp av personalhandläggarna. Uppgifterna läses därefter in i Heroma. För övriga förändringar av löner mm knappas det in manuellt av löneadministratören.

Bedömning
Enligt lönekontoret eftersträvar de att alltid vara två som registrerar förändringar av lön. Det finns dock ingen anvisning kring detta samt att det är svårt att följa upp om så verkligen sker. Dock finns alla beslutande förändringar mm sparade vilket gör att de alltid går att följa upp om något blivit fel. Vår bedömning är att lönekontoret har en hög ambition att förändringar och uppdateringar i systemet ska bli korrekta samt att risken för väsentliga fel är liten. Stora fel skulle sannolikt uppmärksammas vid kontrollen av signallistan.

Rekommendation
Vi anser att det bör göras en rutinöversyn med syfte att säkerställa att förändringar av data sker enligt tvåhandsprincipen. Rutinen bör dokumenteras och skriftligen beslutas.

Revisionsfråga:

7. Registreras och avslutas anställning av annan än den/de som verkställer löne-utbetalning och finns spärrar och/eller kontroller att ”tvåhandsprincipen” följs?

Personaladministratörer och löneadministratörer kan var för sig lägga upp nya personer utan att någon annan involveras. Ett nyupplägg av en person i Heroma medför dock att information om denna person snabbt sprider sig till andra system. Först går uppgifterna till EKO katalogen, där jämförs personuppgifter med uppgifter i befolkningsregistret därefter skapas mejlkonton mm. I framtiden kommer personen även att hamna i den nationella HSA katalogen. Detta gör det ganska svårt att ta bort anställda ur systemen och därmed ökar möjligheten att upptäcka oegentligheter. Faktum är att anställda aldrig raderas ur landstingets lönedatabaser. Efter några år av inaktivitet förs uppgifterna över till en annan databas där de bevaras.

Förändring av personnummer var enligt våra tester inte möjliga att genomföra såvida det inte handlade om ett tillfälligt svenskt personnummer som gjordes om till ett permanent.

Verkställandet av en utbetalning utförs i praktiken av Logica efter godkännande av löneadministrationen, däremot är det de uppgifter som löneadministratören lagt upp som är grund för utbetalningen. Teoretiskt skulle en löneadministratör därför kunna lägga upp t.ex. en närstående och se till att personen får en lön. Däremot kan de inte ändra konteringen av lönen eftersom att de inte har

tillgång till styrregistret. Detta innebär att risken för upptäckt är stor när den som är ansvarig för det kostnadsställe som lönen konterats mot granskar sina kostnader. Det är dock mycket nytt på gång vad gäller denna rutin. När allt kring kopplingen av anställning mot EKO katalogen och HSA katalogen är klar är tanken även att information om nyupplägg av anställning ska via mejl signaleras till närmaste chef.

Bedömning
Grundförutsättningen för att få en lön utbetald är att personen finns med i lönesystemet. Nyupplägg är därmed en kritisk punkt i löneutbetalningskedjan. Ur ett interkontroll perspektiv är det inte acceptabelt att löneadministrativ personal kan lägga upp personer utan någon form av attest eller annan kontroll av chef eller liknande. Den kontroll som idag finns mot att utbetalning av löner sker till felaktiga personer är den analyslista som månatligt skickas ut till den som är ansvarig för det kostnadsstället. Skulle denna person ha dålig kontroll över vilka anställda den har finns risk för felaktiga utbetalningar. Vid ett nyligen upptäckt bedrägeri inom personaladministrationen i ett annat landsting ändrades personnummer på en fd anställd till en närståendes personnummer i samband med lönekörningen. På så sätt väcktes ingen uppmärksamhet över nya personuppgifter i systemet. Vi har testat nämnda förfarande i Heroma utan att lyckas.

Rekommendation
Vi rekommenderar att en undersökning görs om det finns möjlighet att, som en förebyggande åtgärd, se till att det vid varje upplägg av en ny person i löneprogrammet per automatik går ut ett mejl/meddelande till den som ansvarar för det kostnadsställe som angetts i grunduppgifterna. Detta meddelande skulle även fungera som en bekräftelse på att rätt uppgifter kring avtalad lön lagts upp. För att denna kontroll ska fungera får det inte finnas någon som är ansvarig för ett kostnadsställe och som samtidigt kan lägga upp eller begära ett nyupplägg av en ny person i Heroma. Eftersom att den som ansvarar för ett kostnadsställe kan göra denna begäran bör ovan nämnda kontroll kompletteras men att närmaste chef alltid attesterar en begäran om ett upplägg av nya personer. Enligt vad vi erfarit pågår ett arbete med en s.k. EKO-katalog som kommer att underlätta kontrollen över aktualiteten på användaridentiteter och behörigheter, till detta projekt finns även implementering av ”smarta kort” vilket innebär förstärkt id-kontroll vid inloggning.

Vi rekommenderar att det görs en uppföljning när implementeringen av ”smarta kort” och tillhörande rutin för tilldelning är klar

Revisionsfråga:

8. Avstäms utbetalningar mellan lönekontoret och bank på ett tillfredsställande sätt (vilka uppgifter avstäms) och dokumenteras avstämningen?

Vid vårt besök gjordes denna avstämning av systemhandläggarna. Underlag från lönesystem jämfördes med utbetalningslista (SPADAB lista, de uppgifter som skickas till banken för utbetalning) vilket därefter stäms av mot kontoutdrag.

Bedömning
Detta avstämningsarbete får enligt vår mening inte utföras av en person med mycket höga behörigheter. Detta avstämningsarbete är en mycket kritisk punkt vad gäller internkontroll kring löneutbetalningen. Utbetalningslistan erhålls från Logica och denna visar på vad som ska betalas ut per individ. Enligt vår bedömning kan ingen erhålla någon löneutbetalning utan att hamna på denna lista, likaså kan listan inte ändras eller raderas. Då antalet lönekörningar är förbestämda anser vi det vara liten risk att någon lista skulle försvinna obemärkt. Därmed finns ett facit på vilka utbetalningar som skett, vilket kan användas som en upptäckande kontroll. Avstämningsrutinen som sådan, förutom vem som gör den, bedömer vi som tillfredställande.

Rekommendation

Att ovan nämnda avstämningsarbete i fortsättningen sköts av annan person än systemhandläggaren som är väl insatt i kontrollens innebörd och funktion.

Åtgärder från lönekontoret med anledning av våra rekommendationer

Efter att vi lämnat vår rekommendation har löneadministrationen, enligt uppgift, ändrat upplägget avseende avstämningsrutinen mot banken. Numera är det den systemansvarige på löneadministrationen som går igenom förslaget på utbetalningslistan. Den systemansvarige har som nämnts tidigare bara läsbehörighet till lönesystemet varför vår bedömning är att kontrollen är tillfredsställande.

Revisionsfråga:

9. Förekommer extra löneutbetalningar vid sidan av de månadsvisa utbetalningarna och uppfyller rutinerna i så fall kraven på god intern kontroll?

I princip sker utbetalningar varje vecka, dels den stora månatliga utbetalningen men även extra utbetalningar. Dessa går under beteckningen Pluto. Rutinen är i princip densamma som vid de ordinära löneutbetalningarna, den enda skillnaden är att vid dessa löneutbetalningar erhålls utbetalningslistan (SPADAB listan) elektroniskt. Vid den vanliga lönekörningen skickas utskrift från Logica till lönekontoret där den skrivs.

Bedömning
Enligt vår bedömning är det bättre att listan från SPADAB erhålls i filformat eftersom den då är lättare att använda i ett kontrollsyfte. Vi har även testat att radera denna lista men det har visat sig vara omöjligt vilket är bra. Således är den interna kontrollen något bättre vid den tillfälliga utbetalningen. De extra lönekörningarna är precis som för huvudkörningen förbestämda och initieras av Logica. Därmed finns det ingen som på egen hand kan, starta en lönekörning som sedermera generar en utbetalning.

Rekommendation
Som påtalats tidigare rekommenderar vi att avstämningen mellan bankuppgifter och löneutbetalningsuppgifter borde förändras vad gäller bemanning. Det underlag som används vid detta avstämningsarbete bl. a utbetalningslistan från SPADAB, bör vid samtliga lönekörningar även skickas till den systemansvarige elektroniskt eftersom avstämningsarbetet och kontrollen enligt vår rekommendation borde ske där.

Revisionsfråga:

10. Görs en ändamålsenlig avstämning av skuldkonton i ekonomisystemet med avseende på de poster som genereras i lönesystemet och görs en ändamålsenlig avstämning av överförda uppgifter mellan lönesystem och ekonomisystem?

Avstämningen av de lönerelaterade skulderna, semesterlöner, jour- och övertidsskulder, sker genom att ansvarig på ekonomiavdelningen kontaktar lönekontoret för att ur lönesystemet (Heroma) få ut rätt siffror. I Heroma finns alla uppgifter om löner, arbetade övertid, sparade semesterdagar mm. Det är dessa data som Heroma använder i sin beräkning av de lönerelaterade skulderna. Här finns dock problem. Skulden i Heroma stämmer inte överens med saldot i huvudboken. Huvudboken justeras därför för att stämma överens med Heroma. Det verkar dock inte finnas någon enkel förklaring till problemen. Att andra landsting har motsvarande problem indikerar att felet kan finnas i Heroma men det kan även handla om felaktiga uppsättningar och handhavande fel. Systemhandläggarna tror att det t.ex. kan bero på handhavandefel vid semesterkorrigering. De säger även att de fått lägga ner väldigt mycket tid på detta och att de försökt att få Logica att agera. JLL är dock i sammanhanget en liten kund varför det krävs att fler vill få ordning på detta problem. Konkreta exempel på fel som har hittats, är exempelvis semesterskuldsrapporten per person som inte stämmer med det ackumulerade saldot i Heroma. Samt att det använts olika procentsatser när semesterskulden räknats upp kontra när den reducerats. Under hösten 2009 har det gjorts en uppföljning för att se om skillnaderna mellan systemen minskat. Den senaste indikationen från november visar på att differensen nästan försvunnit. Vad gäller själva överföringen av uppgifter, belopp och konteringar, mellan lönesystemet och ekonomisystemet sker det enligt följande. Heroma generar en fil som innehåller alla belopp och hur de har konterats. Därefter läses filen in i Raindance. Avstämning görs egentligen automatiskt men fel kan uppstå. Exempel på fel är att lön bokats på ett stängt kostnadsställe. Felen kommer ut på en fellista, som måste gås igenom och rättas innan de kan bokföras i huvudboken. Rutiner finns för denna avstämning.

Bedömning

Överföringen av uppgifter mellan Heroma och ekonomisystemet (Raindance) borde kunna göras utan att det uppstår differenser, dvs. de borde visa samma siffror. Detta eftersom alla uppgifter i Heroma, inkl förändringar av semesterlöneskulder mm, borde följa med i den ekonomifil som läses över från Heroma till Raindance efter varje lönekörning.

I verkligheten hänger dessa konton dock inte ihop. Det har under flera år förekommit stora differenser mellan dessa system, enligt ansvarig på ekonomiavdelningen rör det sig om uppemot 15 mkr på årsbasis. Beloppet har alltid varit ett överskott, de vill säga de personalrelaterade skulderna, främst semesterlöneskulden har i Heroma konsekvent varit lägre än i Raindance. När skulden i Raindance korrigerats mot uppgifterna i Heroma har det uppstått ett överskott eftersom att skulden minskats. Överskottet har sedermera fördelats ut till olika kostnadsställen utifrån en fastställd modell. Således har det antagits att de ackumulerade saldot, exempelvis för semesterlöneskuld, är korrekt i Heroma. Det som antas blivit fel är uppräkning och uttag av skulden, något som sker vid varje lönekörning. Detta problem är inte JLL ensamma om utan flera av de andra landstingen som också använder Heroma har problem med dessa skuldkonton. Därför bör det finnas bättre påtryckningsmöjligheter för att få detta åtgärdat från leverantören. Svårigheten med att stämma av dessa konton är ett säkerhetsproblem och att det teoretisk innebär att det skulle gå att styra om konteringar mot dessa konton i huvudboken med liten risk för att det skulle uppmärksammas. Det ska dock understrykas att

det idag finns en rutin för att gå igenom dessa konton och identifiera manuella transaktioner som inte borde vara där. Det är förhållandevis lätt att identifiera fel från manuella transaktioner och transaktioner från andra system.
Det ska egentligen bara finnas transaktioner från lönesystemet på dessa konton, men det blir problem om felkonteringen ligger i den lönefil som läses över. Ett sådant fel blir mycket svårt att upptäcka och risken finns därmed att det kan utnyttjas av den som vill mörka en felaktig utbetalning. Som nämnt ovan uppger ekonomiavdelningen att de under hösten fått bukt med detta problem och att avvikelserna numera inte är lika stora. Vi anser dock att åtgärder måste vidtas så att problemet undanröjs helt. Vad gäller själva överföringen mellan Heroma och Raindance kan vi konstatera att när filen från Heroma är inläst i Raindance och alla eventuella felmeddelande korrigerats har alla transaktioner, alla gjorda konteringar med rätt belopp, förts över till Raindance. Vår bedömning är att överföringsrutinen fungerar bra, det finns inbyggda kontroller som förhindrar att fel kan uppstå.

Det kan tyckas motsägelsefullt att det trots allt uppstår differenser. Skillnaderna kommer dock av information som aldrig följer med i filen men som trots allt måste beaktas. Exempelvis kan retroaktiva löneförändringar störa om förändringen på historiskt intjänad övertid inte följer med i den månatliga filöverföringen från Heroma till Raindance.

Rekommendation

Vår rekommendation är därför fortsatt kontakt och påtryckningar mot Heroma. Skillnaden mellan Heroma och Raindance borde inte finnas. Vi är även medvetna om att det arbetas med att komma till-rätta med detta vilket vi anser vara positivt. Det kräver dock support från programleverantören.

Revisionsfråga:

11. Går det i löneprogrammet att styra om mot vilka konton konteringen ska ske, går det exempelvis att styra en löneart till vilket konton som helst i huvudboken?

Enligt våra tester är detta fullt möjligt. Det finns ett styrregister där all uppsättning sker. I styrregistret går det att ändra hur olika lönearter ska konteras. Vidare går det att ändra kostnadsställen. De två systemhandläggarna har behörighet till detta styrregister och vi har inte funnit någon funktion som varnar/flaggar för när detta görs.

Bedömning
Möjligheten att ändra kontering måste finnas- men den får inte innebär även att det får finnas konton och kostnadsställen där fel kan förbli oupptäckta. Med tanke på vad som tidigare nämnts om de personalrelaterade skulderna vill vi hävda att sådana konton finns. Skulle någon med avsikt att gömma en felaktig utbetalning eller ändra styrningen på en löneart till något av dessa konton, är vår bedömning att det skulle vara mycket svårt att upptäcka detta. Därmed uppfylls ett av grund kriterierna som innebär risk för att drabbas av bedrägeri nämligen att det ska finnas ställen att gömma sin motkontering.

Revisionsfråga:

12. Är kontrollen av lönekostnader organiserad på ett ändamålsenligt sätt?

Den kontroll och uppföljning som görs idag är huvudsakligen organiserad på så sätt att resp kostnadsställeansvarig månatligen får en analyslista. Kontrollen bygger på att de kostnadsställeansvariga går igenom analyslistan och att de reagerar på ev. felaktigheter.
Omvänt kan man teoretiskt säga att om någon kostnadsställeansvarig konsekvent skulle underlåta att utföra denna kontroll , så uppstår en risk att oegentligheter kan passera obemärkt.

Bedömning
Rutinen som sådan är bra men vi rekommenderar dock att den förbättras genom att de kostnadsställeansvariga åläggs att bekräfta riktigheten i gjorda nyupplägg och förändringar av fast data, exempelvis ändrad lön. Detta bör helst göras genom någon form av automatisk kontroll. Exempelvis att ett nyupplägg i Heroma alltid måste godkännas direkt i programmet av annan än den som gjort upplägget. Om detta inte är möjligt föreslår vi att landstinget undersöker om det skulle vara möjligt att ta fram en lista, över gjorda nyupplägg och förändringar i fasta data, som alltid följer med vid utskicket av analyslistan till de kostnadsställeansvariga som underlag för deras kontroll.

Revisionsfråga:

13. Har det gjorts någon kartläggning och riskbedömning av ”hela” lönehanteringen, manuella rutiner, datasystem och dess samband mot ekonomi?

Enligt lönekontoret finns det ingen aktuellt dokumentation som beskriver hela lönehanteringen med rutiner, datasystem mm. Det finns ett dokument angående ”Kris och säkerhet” från 2004 men inget heltäckande dokument har kunnat presenteras för oss.

Bedömning
Enligt 1 kap. 7§ Lag om kommunal redovisning ska det finnas en systemdokumentation avseende samlingsplan, behandlingshistorik och verifieringskedja. Det måste därmed göras en rutinbeskrivning över hur hela lönerutinen går till, från upplägg av anställd till avstämning av banktransaktion mot löneutbetalning. Det finns idag ingen uppdaterad fullständig version av denna rutin. En bra rutinbeskrivning är ett bra hjälpmedel för att underlätta arbetsrotation samt för att minimera risken att kunskap går förlorad om någon hastigt försvinner ur organisationen.

Rekommendation
Vi anser att en rutinbeskrivning över löneprocessen måste tas fram.

Revisionsfråga:

14. Förekommer rotation på arbetsuppgifter inom lönekontoret? Finns tillräcklig backup för nyckelbefattningar inom lönekontoret och förekommer rotation av arbetsuppgifter på dessa befattningar?

Enligt lönekontoret finns det två grupper, med 3 personer i varje grupp, som arbetar med lönerna. Det finns ingen person som besitter någon unik kunskap och det finns ingen arbetsuppgift som bara en person kan. Vilka anställda man beräknar lönen för varierar inom gruppen. På systemsidan finns två personer som kan lika mycket.

Bedömning
Enligt de uppgifter som erhållits, förefaller arbetsrotation och backup vara tillräckliga. Uppgifterna är dock svåra att verifiera.

7.3 SLUTSATS

Det kan tyckas vara en omöjlig uppgift att täcka alla tänkbara sätt att manipulera en lönerutin. I grunden handlar dock allt om att förhindra att otillåten utbetalning kan ske. Utgångspunkten ska därmed vara hur man ska förhindra att någon ger sig själv eller en medbrottsling en otillåten utbetalning. Alla andra åtgärder handlar om att utbetalningen ska kunna upptäckas när den väl inträffat. Om det dessutom finns ett konto där det går att gömma motbokningen, den skuld eller kostnad som utbetalningen ger upphov till, finns det en risk för att ett svindleri skulle kunna genomföras.

Nedan finns en illustration över tre grundkriterier för att lyckas med ett svindleri
.

En kontrollåtgärd som förhindrar någon från att göra fel, medvetet eller omedvetet, är alltid mer effektiv än en kontroll som handlar om att upptäcka fel. Om den förhindrande kontrollen dessutom byggs in i systemet blir den ännu bättre. Förhindrande kontroller kan dock i praktiken vara omöjliga att applicera på alla processer. När så är fallet bör det kompenseras av ökade kontroller av upptäckande art. Om upptäcktskontrollerna är tillräckligt bra fungerar de även i ett avskräckande syfte.

I detta fall handlar de förhindrande åtgärderna om att ingen ska kunna betala ut en lön till sig själv eller till någon medbrottsling eller liknande. För att kunna få en utbetalning krävs att man finns upplagd i lönesystemet. Den kritiska information som skickas till banken vid utbetalning är belopp och personnummer. Med andra ord är den kritiska faktorn att ingen ska kunna boka upp lön på sitt eget personnummer och inte heller felaktigt kunna boka upp lön på någon annans personnummer utan upptäckt.

För samtliga användare av lönesystemet, exkl systemhandläggarna, var det egna personnumret spärrat. Att lägga till spärren var dock en manuell hantering som sköts av systemhandläggarna. Att det överhuvudtaget fanns möjlighet att välja om spärren skulle aktiveras eller ej innebar en väsentlig

säkerhetsrisk. Efter vår rekommendation ändrades behörigheterna och numera kan systemhandläggarna inte längre ändra sin egen lön via Heroma.

För övrig löneadministrativ personal är det egna personnumret spärrat. Därmed reduceras förskingringsrisken till att någon lägger upp en medbrottsling i lönesystemet alternativt ändrar ett befintligt personnummer till sin medbrottslings eller t.ex. ens barn. Vi har försökt att ändra personnummer i systemet utan att lyckas och således kvarstår bara att lägga upp en falsk person i lönesystemet. För upplägg av nyanställda är tvåhandsprincipen önskvärd. En variant skulle kunna vara att den person som anges som den anställdes chef/ansvarig för kostnadsstället även attesterar nyupplägget. I det fall det är personen som ansvarar för kostnadsstället som begär ett upplägg bör istället dennes chef attestera begäran.

Under vår granskning framkom även att systemhandläggarna, via programmet QM, har möjlighet att arbeta direkt mot databasen via SQL kommandon. Det som är problemet, ur ett internkontrollperspektiv, är att den som arbetar direkt med SQL eller QM mot databasen oftast undgår de kontroller som finns i applikationen. Det svårt för oss att bedöma vad som går att utföra med detta verktyg vid löneadministrationen, generellt kan dock sägas att en person kunnig i SQL och med kunskap om tabellverket i teorin kan göra vad som helst. Att viss supportpersonal med höga behörigheter måste finnas är oundvikligt. De personer som har en sådan behörighet utgör dock en potentiell risk. För att bibehålla en god intern kontroll rekommenderar vi dock att kontroller av upptäckande art förstärks kring personer med höga behörigheter. Det som kan ha en preventiv effekt är skyddade loggar och särskild granskning av utbetalningar till personer med höga behörigheter.

En brist som identifierats är att det i teorin även finns personer med höga behörigheter hos systemleverantören. I samband med vår granskning har det framkommit att personalen vid Logica loggar in på Heromaservrarna med en gruppanvändaranvändaridentitet och ett lösenord. Gruppanvändaranvändaridentiteten ger full behörighet på de servrar där Heroma är installerade. Med detta följer även en möjlighet att radera loggar. Således går det att gå in i systemet, utföra ändringar och radera alla spår efter åtgärden. För att god intern kontroll ska anses föreligga anser vi att gemensamma användarkonton inte får finnas för personer med möjlighet att utföra ändringar i systemet. Vidare bör löneadministrationen ställa krav på att externa leverantörer styrker att de har en tillräcklig säkerhet innan de ges behörighet att logga in på landstingets servrar.

Ett problem som finns är svårigheten att identifiera felaktiga konteringar på jour-, övertid och semesterskuldskontona. Detta problem uppstår i Heroma men överförs till Raindance. Eftersom det råder oklarheter kring beräkningarna av de personalrelaterade skulderna samt det faktum att Raindance korrigeras mot Heroma för att få det att överensstämma är möjligheten för att upptäcka ett medvetet fel litet. Detta tillsammans med det faktum att det via styrregistren går att ändra förbestämda konteringar gör att det i teorin går att motboka en medvetet felaktig transaktion på dessa konton med liten risk för upptäckt. Det bör dock påpekas att ekonomiavdelningen under hösten ansett att de nu fått bukt med detta problem och att avvikelserna numera inte är lika stora.

Sammanfattningsvis kan vi konstatera att det innan våra rekommendationer beaktades, i teorin och för några få individer, fanns möjlighet att göra otillåtna löneutbetalningar. Genom några få insatser anser vi att lönekontoret redan minskat risken för att detta ska vara möjligt att genomföra. Ytterligare insatser finns att göra, bland annat vidta åtgärder för att höja sannolikheten för att felaktigheter upptäcks, förbättra dokumentationen kring utgivna behörigheter, inför stärkt identitetskontroll för inloggning till landstingets servrar för externa leverantörer, ökade kontroller av utbetalda löner till personer med hög

behörighet och aktiv uppföljning av loggar samt se till att de inte går att radera. Genomförs dessa förändringar anser vi att lönekontoret kan uppnå en godtagbar intern kontroll.

Löneadministrationen har, i positiv anda, redan under våra intervjuer tagit fasta på en del av våra rekommendationer. Några har lett till förändringar som redan är implementerade. Några kräver hjälp av systemleverantören, Logica, medan en del andra förslag är på gång genom andra projekt. De projekt som är på gång rör bland annat tidigare nämnda EKO-katalog, ny rutin för behörighetstilldelning, användning av smarta kort vid inloggning till dator.

Umeå den 10 december

Jonas Wiberg
Revisor