Bilaga 1

Riksrevisionen - Kronofogden

Granskning med fokus på IT-risker

23 januari 2013

ERNST & YOUNG

Innehållsförteckning

Granskning utförd av: Ernst & Young AB
Granskningsperiod: oktober 2012 - januari 2013

Mottagare:

- Lars Nordstrand — Riksrevisionen
- Emma Karlemo — Riksrevisionen

1. Sammanfattning

Riksrevisionen har inom ramen för 2012 års revision av Kronofogden (KFM) uppdragit åt Ernst & Young att genomföra en granskning av den interna kontrollen kring systemet REX. Syftet med granskningen är att undersöka huruvida den interna kontrollen i det IT-system som stödjer de finansiella processerna uppbördshantering och medelshantering är ändamålsenligt utformade. Uppdraget omfattar en kartläggning av KFM:s befintliga processer för programförändringar, behörighetshantering och driftsrutiner för systemet REX, samt identifiering och testning av utvalda nyckelkontroller i dessa processer. Kartläggningen innefattar även granskning av kontroller som syftar till att säkerställa integriteten i översättnings-tabellen mellan medelslag i REX och huvudbokskonton i Agresso.

Systemet REX förvaltas av Skatteverket (SKV). Kartläggningen av processerna genomfördes därför genom intervjuer med personal från både KFM och SKV samt granskning av tillhandahållen dokumentation. Utifrån kartläggningen identifierade vi nyckelkontroller i processerna och utförde test av ett lämpligt urval av kontrollerna.

Då REX ägs av KFM men förvaltas av SKV finns ett serviceavtal mellan myndigheterna som reglerar grundläggande delar av ansvarsrelationen och servicenivåer för systemet. Avtalet omfattar även regler för hur KFM kan avropa beställningar av programförändringar mot SKV. Detta ansvarsförhållande har lett till att spårbarheten i programförändringsprocessen varit högre än för andra processer. Vi har dock noterat vissa brister kring hur KFM utformar och följer upp kravställningen i avtalet mot SKV. Detta innebär bland annat otydliga krav på säkerhetskopiering och återläsningstest. Vi har också noterat att KFM har kontroller på plats för att godkänna och följa upp behörigheter i REX, men att dessa inte är tillräckliga för att förhindra att inaktuella behörigheter finns kvar samt att spårbarheten i kontrollerna kan förbättras.

Vår sammanfattande bedömning är att KFM i flera avseenden har ändamålsenligt utformade kontroller men att det i vissa avseenden finns utrymme för förbättring. Vid vår granskning har vi noterat ett antal iakttagelser och gett rekommendationer för hur dessa kan åtgärdas:

- Inaktuella användare med höga behörigheter förekommer
- Regelbundna genomgångar av användare är inte ändamålsenligt utformade
- Test av programförändringar genomförs inte alltid
- Avsaknad av specifikation kring säkerhetskopiering och återläsningstester
- Begränsad spårbarhet i processen för behörighetshantering

En fullständig redogörelse för våra iakttagelser och rekommendationer återfinns i avsnitt 5.

2. Inledning

2.1 Uppdragsbeskrivning

Riksrevisionen (RiR) har inom ramen för 2012 års revision av Kronofogden (KFM) uppdragit åt Ernst & Young (EY) att genomföra en granskning av den interna kontrollen kring systemet REX. Syftet med granskningen är att undersöka huruvida den interna kontrollen i de IT-system som stödjer de finansiella processerna uppbördshantering och medelshantering är ändamålsenligt utformade.

Uppdraget omfattar en kartläggning av KFM:s befintliga processer för programförändringar, behörighetshantering och driftsrutiner för systemet REX, samt identifiering och testning av kontroller i dessa processer. Kartläggningen innefattar även kontroller för att säkerställa integriteten i översättningstabellen mellan medelslag i REX och huvudbokskonton i Agresso.

Uppdraget är ett avrop på ramavtalet med dnr 38-2008-0904. Avropet har dnr 38-2012-1289.

2.2 Bakgrund

KFM är en myndighet med uppdrag att skapa balans mellan fordringsägare och gäldenär. Myndighetens huvudsakliga uppgifter består av indrivning av obetalda fordringar, utfärdande av betalningsföreläggande, beslut om skuldsanering samt att agera tillsynsmyndighet för konkursförvaltare. KFM var tidigare en del av Skatteverket (SKV) men sedan 2008 verkar myndigheten självständigt under Finansdepartementet.

Företags och enskildas ekonomiska förehavanden är känslig information vilket ställer höga krav på god intern kontroll inom IT-miljön för att verksamheten ska kunna bedrivas ändamålsenligt.

2.3 Genomförande

Uppdraget genomfördes under perioden oktober 2012 - januari 2013. Information samlades in dels genom intervjuer med personal från både KFM och SKV, dels genom granskning av tillhandahållen dokumentation. Se bilaga A för en översikt över respondenter och granskade dokument. Uppdraget genomfördes i följande tre steg:

- Kartläggning av processerna för programförändring, behörighetshantering och driftrutiner i REX samt behörighetshantering i översättningstabellen mellan REX och Agresso
- Identifiering av nyckelkontroller i processerna
- Test av ett lämpligt urval av identifierade kontroller

2.4 Omfattning och avgränsning

Detta dokument beskriver vår granskning av processerna för hantering av programförändringar, behörigheter och driftsrutiner i systemet REX samt integriteten i översättningstabellen mellan REX och Agresso. De driftsrutiner som omfattas av granskningen är rutiner för säkerhetskopiering och återläsningstester.

Vår granskning har inte haft sådan omfattning eller inriktning att vi har haft möjlighet att upptäcka alla brister, oegentligheter eller andra avvikelser som kan förekomma. Kontroller och rutiner kan heller aldrig utgöra ett fullständigt skydd mot försummelser eller mot oegentligheter som utförs av flera personer i samarbete.

3. Granskning av processerna kring REX

Rex är KFM:s system för indrivning och redovisning. Systemet, som drivs i stordatormiljö, stödjer KFM:s processer för handläggning av allmänna och enskilda mål. Rex är egenutvecklat och togs i drift på 1970-talet. KFM har under en längre period planerat att byta ut systemet och vissa delar håller successivt på att avvecklas. Det är dock osäkert när hela systemet kommer att vara utbytt. Planerna innebär att utvecklingen av REX främst fokuserats till att främja en framtida avveckling av systemet.

Förvaltningen av REX sköts i dagsläget av SKV som även hanterar driften av övriga IT-system på KFM. Detta är en följd av att KFM tidigare var en del av SKV. Driften regleras av ett serviceavtal myndigheterna emellan. SKV anlitar i sin tur IT-företaget Logica för den praktiska driften av IT-systemen på de båda myndigheterna.

3.1 Programförändringar

Eftersom REX är på väg att fasas ut är utgångspunkten gällande programförändringar att utveckla så lite som möjligt. Den utveckling som görs ska i så stor utsträckning som möjligt göras i syfte att underhålla systemet samt anpassa systemet för avveckling. Samtliga programförändringar som görs i REX utvecklas på SKV där utvecklingsavdelningen sitter. Det förekommer två huvudtyper av programförändringar i REX:

- **Större förändringar** - görs i projektform och syftar oftast till att avveckla REX
- **Mindre förändringar** – görs i form av avrop på tjänsteavtalet mellan KFM och SKV

Större förändringar
Större förändringar hanteras i projektform och genomförs numera främst i syfte att avveckla REX. De förändringar som genomförs på detta sätt syftar till att anpassa REX till ersättande system för att möjliggöra exempelvis nödvändig informationshämtning under den period som systemen körs parallellt. Processen för förändringshanteringen finns beskriven i ett dokument gemensamt för KFM och SKV.

Förändringen initieras formellt i systemet KOLL där KFM lägger en offertförfrågan. Efter diskussioner om behov, lösningsförslag och kostnad är det upp till KFM:s beställare att fatta beslut om huruvida en beställning ska läggas eller inte.[1] Om lösningsförslaget innebär en kostnad på över 0,5 MSEK ska det kvalitetssäkras av ytterligare en person på SKV innan det presenteras. För varje förändringsprojekt ska SKV även ta fram en omfattningsbeskrivning och en projektplan.

När beställningen lagts inleder SKV:s projektgrupp utvecklingsprojektet. Efter utvecklingsperioden följer en testperiod där regressions- och systemintegrationstester genomförs enligt en testplan och dokumenteras som beslutsunderlag inför produktionssättning.[2] Det finns inga fastställda rutiner för genomförande av acceptanstester, något som bör göras av beställaren, i det här fallet KFM, i syfte att

[1] Kontroll nr. 1 enligt *Tabell 1* nedan.
[2] Kontroll nr. 2 enligt *Tabell 1* nedan.

utvärdera hur väl den färdigutvecklade programförändringen uppfyller de ställda kraven.

Inför produktionssättning sammanställer den rådgivande gruppen D-CAB (driftens Change Advisory Board) en statusrapport och stämmer av att samtliga krav är uppfyllda. Statusrapporten används sedan som beslutsunderlag av SKV:s IT-avdelning i sitt beslut om att lämna en rekommendation om produktionssättning.[3]

Produktionssättning av förändringen genomförs under ledning av uppdragsledaren för REX. Efter detta följer en interimsperiod som avslutas med att eventuella kvarstående defekter åtgärdas av utvecklarna.

Mindre förändringar
Mindre förändringar görs som avrop på ett tjänsteavtal som KFM har med SKV. Förändringen initieras formellt med en beställning som KFM gör i systemet E-beställ som är gemensamt för KFM och SKV och tillhandahålls av Logica[4]. Beställningen föregås dock ofta av en diskussion mellan beställaren på KFM och utvecklarna på SKV. Endast behörig personal på KFM kan göra e-beställningar. Alla beställningar går till uppdragsledaren för REX på SKV som därefter kontaktar beställaren. Via e-post och telefon kan nu kompletteringar göras i beställningen och en utförlig uppdrags-beskrivning dokumenteras. Uppdragsledaren sparar alla dokument gällande en beställning i en avropspärm.

Alla förändringar produktionssätts av uppdragsledaren för REX. Innan dess genomförs i vissa fall tester av utvecklaren. Beslut om huruvida en utveckling ska testas innan den produktionssätts fattas av den utvecklare som ansvarat för förändringen efter diskussion med uppdragsledaren. Acceptanstester genomförs aldrig av KFM för denna typ av programförändring.

Varje månad skickar SKV en månadsrapport till KFM med servicenivåer och leveranser där de avrop som har gjorts på tjänsteavtalet finns sammanställda.[5]

Kontroller i processen för hantering av programförändringar
I tabell 1 presenteras de kontroller som vi har identifierat i processen för hantering av programförändringar i REX samt en bedömning av huruvida kontrollerna är ändamåls-enligt utformade. Vi har gjort en gemensam bedömning för processerna för hantering av större och mindre förändringar.

Kontroll-nummer	Kontrollbeskrivning	Kontrollen är ändamålsenligt utformad	Kommentar från test av kontroller
1	Endast godkända förändringar genomförs.	[illegible]	Vid granskningen fick vi ta del av dokument från en större och en

[3] Kontroll nr. 3 enligt *Tabell 1* nedan.
[4] Kontroll nr. 1 enligt *Tabell 1* nedan.
[5] Kontroll nr. 5 enligt *Tabell 1* nedan.

Kontroll-nummer	Kontrollbeskrivning	Kontrollen är ändamålsenligt utformad	Kommentar från test av kontroller
2	Förändringar testas innan de överförs till produktionsmiljön.	Nej*	mindre förändring. Ur dessa kunde vi utläsa att båda förändringarna hade en formell beställning och en ansvarsfördelning gällande beställning och produktions-sättning. Däremot saknades testdokumentation och formellt beslut om produktionssättning för den mindre förändringen.
3	Testresultat godkänns innan förändring produktionssätts.	Nej**	
4	Det finns ansvarsfördelning i programförändringsprocessen, dvs. det är inte samma person som skapar en förändring som produktionssätter den.	Ja	
5	SKV gör en månatlig sammanställning av alla aktuella mindre förändringar. Denna skickas till KFM.	Ja	Vid granskningen fick vi ta del av en sammanställning som skickats till KFM. Denna kontroll gäller endast mindre förändringar som är fler till antalet än de större.

Tabell 1: Kontroller i processen för hantering av programförändringar i REX

**) I processen för större förändringar genomförs och dokumenteras regressions- och system-integrationstester, dock inte acceptanstester.*
***) I processen för större förändringar godkänns testresultaten innan förändringen produktions-sätts. Eftersom detta inte gäller för mindre förändringar bedöms kontrollen vara icke ändamåls-enligt utformad.*

3.2 Behörighetshantering

Behörighetshanteringen av handläggarbehörigheter i REX administreras av en central grupp på SKV, gruppen för behörighetsadministration. Handläggarbehörigheter i REX styrs genom systemet NBKS (Nya Behörighetskontrollsystemet) vilket också används för att administrera behörigeter för andra system än REX både på KFM och SKV. Höga behörigheter direkt till stordatormiljön tilldelas genom behörighetssystemet RACF och hanteras inte av behörighetsadministrationen utan av en särskild förvaltningsgrupp på SKV.

För närvarande pågår flertalet initiativ för att öka säkerheten gällande behörigheter inom KFM. Detta beror delvis på att KFM börjat bygga upp en egen säkerhets-organisation efter att tidigare varit sammankopplad med SKV och att ansvaret för säkerheten tidigare har legat på SKV. Ett av de initiativ som tagits på KFM i syfte att upprätta en egen säkerhetsorganisation är införandet av ett så kallat Behörighets-forum. En pilotstudie genomfördes under våren 2012 och beslut om införande fattades den 11 oktober. Forumet ska fungera som ett stöd i behörighetsfrågor där kompetenser från olika delar av verksamheten medverkar. Genom Behörighetsforum ska kopplingen mellan verksamhetens behov, tekniska möjligheter och de juridiska och ekonomiska frågor som inverkar förtydligas. Rent praktisk ska alla förändringar av behörigheter på KFM beredas i Behörighetsforum för att sedan beslutas av system-ägaren eller informationsägaren.

Roller

KFM har tre huvudgrupper av behörigheter:

- **grundbehörigheter** - innefattar grundläggande IT-funktioner som nätverkskonto
- **enkla behörigheter** - innefattar behörigheter som ger åtkomst till information i verksamhets- och stödsystem inom KFM
- **särskilda behörigheter** - innefattar behörigheter som KFM har bedömt vara känsliga

Särskilda behörigheter innefattar specifikt tre typer av behörigheter som ska hanteras med extra försiktighet:

- behörigheter som ger åtkomst till känsliga personuppgifter
- behörigheter som kan godkänna eller ändra större ekonomiska transaktioner
- behörigheter som ger system- eller behörighetsadministratörsrättigheter

Majoriteten av behörigheterna i REX är av typen enkel behörighet och ett fåtal är av typen särskild behörighet.

På KFM tilldelas användarna i verksamhets- och stödsystem behörigheter genom behörighetsprofiler som ska motsvara användarens arbetsuppgifter. En behörighetsprofil består av en uppsättning behörighetsroller från olika system, av vilka REX är ett. I de fall då en lämplig behörighetsprofil inte går att applicera på en användare kan individuella tilläggsbehörigheter tilldelas. På detta sätt kan en för snäv behörighetsprofil utvidgas i stället för att en för omfattande profil tilldelas. Det finns även tilläggstjänster som kan tilldelas som ligger utanför NBKS.

Upplägg eller ändring av användare

Beroende på behörighetstyp (grund-, enkel eller särskild behörighet) skiljer sig förfarandet vid upplägg eller ändring av användare något. Grundbehörigheter tilldelas som en del i det startpaket som varje nyanställd får och kräver inget särskilt godkännande medan enkla behörigheter kräver ett formellt tilldelningsbeslut. Särskilda behörigheter innebär ytterligare krav då ett så kallat dubbelt godkännande krävs. För den typen av särskild behörighet som ger åtkomst till känslig personinformation eller ger möjlighet att godkänna eller ändra större ekonomiska transaktioner krävs godkännande från personalansvarig chef och verksamhetschef. För särskild behörighet som ger system- eller behörighetsadministratörsrättigheter krävs godkännande från personalansvarig chef och informations- eller systemägare.

KFM tillämpar en process vid upplägg eller ändring av användare där närmaste chef ansvarar för att varje medarbetare i den egna personalen har rätt befogenheter i systemen och endast har tillgång till information nödvändig för att kunna utföra arbetet. Närmaste chef fyller i en e-blankett där åtgärd anges, dvs. om det handlar om ett nyupplägg eller en ändring, vilken behörighetsprofil användaren ska ha samt om några tilläggsbehörigheter eller tilläggstjänster ska läggas upp. Blanketten skrivs ut och signeras av chefen samt användaren i de fall åtgärden är en behörighetsändring[6]. Handlar det om särskilda behörigheter ansvarar chefen för att en andra attest ges av

[6] Kontroll nr. 1 enligt *Tabell 2* nedan.

rätt person. Blanketten skickas sedan per brev till behörighetsadministratörerna på SKV som granskar blanketten och lägger upp aktuella behörigheter. Vid felaktigheter skickas ärendet tillbaka till beställande chef för komplettering. Originalblanketten skickas avslutningsvis till KFM:s behörighetssamordnare som ansvarar för arkivering av blanketten.

Den arkiveringsrutin som idag tillämpas på KFM innebär att KFM:s behörighets-samordnare arkiverar samtliga behörighetsblanketter centralt. Denna rutin infördes i slutet av 2011. Innan dess hanterade personalcheferna arkiveringen av sina egna respektive blanketter. Behörighetssamordnaren har i dagsläget mottagit blanketter för ett antal år tillbaka från ett fåtal av personalcheferna och arkivering av dessa pågår. Med anledning av detta finns en begränsad spårbarhet bland beställningarna av behörigheter.

Borttag av användare
Borttag av användare i REX följer samma rutin som för upplägg eller ändring av användare. Ansvarig chef fyller i en blankett där åtgärden *Avslut av konto* väljs. Detta föranleder att kontot spärras efter sju dagar och avslutas efter sex månader.[7] I och med det faktum att alla behörigheter läggs upp på en maximal period på två år undviks att behörigheter ligger kvar i REX långt efter att en användare har lämnat KFM även om processen för borttag av användare skulle förbigås.

Regelbundna genomgångar av befintliga användare
Alla behörigheter som läggs upp i REX är tidsbegränsade till att gälla innevarande år och nästa. Således är behörigheterna aldrig aktiva i mer än två år. Varje år görs under hösten en genomgång av samtliga användare då alla personalansvariga chefer måste fylla i en blankett för var och en av sina anställda i vilken de kan göra eventuella behörighetsändringar, ta bort användaren eller bekräfta att behörigheterna ska gälla även nästa år[8]. Det finns inget sätt att dra ut en lista med samtliga användare i REX varför de som gör genomgången av användare får utgå från aktuella personallistor.

Genomgången för 2012 startades den 1 oktober 2012 då instruktioner om genom-gången lades upp på KFM:s intranät. Genomgången pågår fram till årsskiftet då alla behörigheter som inte har förnyats inaktiveras. Det finns användare i REX som är anställda på SKV och som därmed inte omfattas av KFM:s årliga genomgång. Dessa täcks emellertid in av den årliga genomgång som SKV gör av sina anställda. Under 2012 kommer SKV dock inte att göra någon genomgång på grund av implemen-teringen av ett större projekt. Samma scenario gällde för KFM år 2011 varför ingen årlig genomgång på KFM gjordes då. Detta innebär att en genomgång av befintliga användare i REX som omfattar samtliga användare inte har gjorts på två år.

Höga behörigheter
Höga behörigheter är de som utvecklare och driftpersonal behöver för att administrera REX. Dessa användare sitter i förvaltningsgruppen för REX på SKV och kan logga in direkt i stordatormiljön. Även personal från Logica har höga behörigheter

[7] Kontroll nr. 2 enligt *Tabell 2* nedan.
[8] Kontroll nr. 3 enligt *Tabell 2* nedan.

för att kunna hantera driften av systemet. Behörigheterna styrs i behörighetsmodulen RACF.

Den högsta typen av behörigheter är så kallade *superusers* som endast innehas och administreras av personal på Logica. Höga behörigheter som innehas av personal på SKV tilldelas genom vissa fördefinierade roller beroende användarens arbetsuppgifter är (t.ex. *ÅREX, DO44DRIF, DO44SERV* och *DO44DAFA).*

I grupperna med höga behörigheter finns användarkonton tillhörande den person på SKV som arbetar med administrationen av REX samt det tiotal användare som arbetar med utvecklingen av REX. Utöver dessa finns konton tillhörande personal från Logica och ett antal konton som inte längre används. Dessa har tillhört användare som antingen slutat på SKV eller bytt tjänst.

För att logga in i stordatormiljön krävs ett personligt identitetskort som förs in i datorn. Vid första inloggningstillfället sparas lösenordet på kortet och byts sedan automatiskt var 27e dag. Det finns ingen process för upplägg eller borttag av användare med höga behörigheter i RACF. Systemadministratören lägger upp behörigheter vid behov och tar bort dem i de fall då information skickas om att så ska göras. Vid upplägg eller borttag av höga behörigheter för anställd på SKV finns det emellertid en odokumenterad rutin. Rutinen består i att chefen för förvaltningsgruppen skickar ett e-brev till administratören av RACF som därefter hanterar ärendet. Denna rutin omfattar inte övriga användare med höga behörigheter i RACF.

Det görs ingen regelbunden genomgång av användarna i RACF och de regelbundna genomgångar som görs på KFM av användarna i NBKS omfattar inte kontona i RACF. Detta resulterar i att gamla konton med höga behörigheter kan ligga kvar efter att de slutat användas, något som är fallet i vissa av grupperna. Detta innebär att det är upp till förvaltaren av varje behörighetsroll att själva se över och hålla användare som har rollen uppdaterade, detta sker i varierande grad beroende på vilken roll det gäller.

Kontroller i processen för behörighetshantering

I tabell 2 presenteras de kontroller som vi har identifierat i processen för behörighetshantering i REX samt en bedömning av huruvida kontrollerna är ändamålsenligt utformade.

Kontroll-nummer	Kontrollbeskrivning	Kontrollen är ändamålsenligt utformad	Kommentar från test av kontroller
1	Behörigheter beställs och godkänns skriftligen av behörig person i samband med tilldelning eller vid förändring av behörigheter då personal börjar eller byter arbetsuppgifter.	Ja	Eftersom det inte är möjligt att dra ut en fullständig lista från REX med samtliga användare fick vi vid granskningen ta del av utvalda listor över de behörigheter som KFM har bedömt vara känsliga. På grund av att arkiveringen av behörighetsbeställningar fram till slutet av 2011 varit decentraliserad kunde vi inte ta del av beställningsunderlaget för utvalda användare.
2	Behörigheter tas bort eller inaktiveras i systemet då personal slutar på avdelningen.	Ja	

Kontroll-nummer	Kontrollbeskrivning	Kontrollen är ändamålsenligt utformad	Kommentar från test av kontroller
3	Behörigheter granskas regelbundet och inaktuella eller felaktiga behörigheter korrigeras.	Nej	Eftersom 2012 års genomgång pågick vid granskningen kunde vi inte ta del av resultatet av denna. Vi kunde däremot bekräfta att den pågick. Granskningen utgår inte från en systemgenererad lista över fullständiga behörigheter i systemet. Istället utgår den från att chefer granskar behörigheter för sin personal, detta innebär att inaktuella konton i systemet kan ligga kvar utan att upptäckas vid granskningen.
4	Det finns ansvarsfördelning i processen för att lägga till eller ändra behörigheter, dvs. det är inte en och samma person som ansöker, godkänner och tilldelar behörigheter till systemen.		Eftersom det inte är möjligt att dra ut en fullständig lista från REX med samtliga användare fick vi vid granskningen ta del av utvalda listor över de behörigheter som KFM har bedömt vara känsliga. På grund av att arkiveringen av behörighetsbeställningar fram till slutet av 2011 varit decentraliserad kunde vi inte ta del av beställnings-underlaget för utvalda användare. Således kan vi inte bedöma huruvida kontrollen utförts regelmässigt eller inte.
5	Tillgång till privilegierade rättigheter är begränsad till lämpliga individer.	Nej	Vid granskningen kunde vi bekräfta att det förekom inaktuella konton i ett urval av de grupper som innefattar höga behörigheter.

Tabell 2: Kontroller i processen för behörighetshantering i REX

3.3 Säkerhetskopiering och återläsningstester

I KFM:s interna styrdokument beskrivs riktlinjer för både säkerhetskopiering och återläsningsrutiner (benämnt återstartsrutiner i KFM:s dokument) för KFM:s system. Enligt riktlinjerna ska såväl säkerhetskopiering som återläsningstester genomföras regelbundet på verksamhetsinformation och program. Det är systemägaren för respektive system som ansvarar kravställning och uppföljning av detta. I ansvaret ingår fastställandet av hur ofta och på vilket sätt säkerhetskopior ska tas samt hur de ska förvaras.

Eftersom driften av KFM:s system köps in från SKV enligt ett serviceavtal myndigheterna emellan är det SKV som hanterar säkerhetskopiering och återläsningstester på KFM. SKV i sin tur köper in dessa tjänster enligt ett serviceavtal som myndigheten har med Logica. I avtalet som KFM har med SKV specificeras bl.a. servicenivån av REX som hög vilket innebär att 99 % av servicetiden ska vara avbrottsfri. Avtalet specificerar emellertid inte med vilken frekvens SKV (i förlängningen Logica) ska genomföra säkerhetskopiering och hur länge dessa ska förvaras. Avtalet anger heller

inga krav på hur återläsningstester av information från REX skall genomföras eller med vilken frekvens.

I tabell 3 presenteras de kontroller som vi har identifierat i processen för säkerhetskopiering och återläsningstester i REX samt en bedömning av huruvida kontrollerna är ändamålsenligt utformade.

Kontroll-nummer	Kontrollbeskrivning	Kontrollen är ändamålsenligt utformad	Test av kontroll
1	KFM har kravställt hur verksamhetsinformation och program skall säkerhetskopieras regelbundet för att vara möjliga att återläsa.	Nej	Vid granskningen fick vi ta del av det serviceavtal som KFM har med SKV. I detta noterade vi att det inte finns några krav i avtalet med SKV i vilken omfattning säkerhets-kopiering eller återläsningstester skall ske.
2	KFM har kravställt hur återläsningstester för verksamhetsinformation och program skall genomföras.	Nej	

Tabell 3: Kontroller i processen för säkerhetskopiering och återläsningstester av REX

4. Granskning av hanteringen av översättningstabellen mellan REX och Agresso

Översättningstabellen mellan REX och Agresso är en tabell som används för att översätta interna konton i REX till huvudbokskonton i Agresso. Den innehåller information om så kallade medelslag som anger på vilka konton olika poster ska bokföras. Tabellen används en gång in månaden i samband med bokslut och redovisningsfilerna överförs som schemalagda jobb som sparas på en yta från vilken en agent i Agresso sedan läser in. Om något i överföringen går fel skickas ett e-postmeddelande till den person på KFM som ansvarar för tabellen.[9]

Det är endast utvecklingsavdelningen på SKV som har tillgång till att göra ändringar i tabellen. Tabellen uppdateras sällan och då är det vanligen i samband med en ny lagstiftning då ett medelslag har ändrats. Den senaste ändringen gjordes för mer än ett år sedan och var av denna typ.

Eftersom det är utvecklingsavdelningen som hanterar ändringar i tabellen sköts dessa som programförändringar och specifikt som förändringstyp 2 som beskrivs i stycket om programförändringar ovan. Avrop görs på ett tjänsteavtal som KFM har med SKV efter att KFM har gjort en beställning i systemet E-beställ[10]. I förändringsspecifikationen får sedan beställaren på KFM besvara en rad fördefinierade frågor för att tydliggöra för utvecklarna vad som ska åtgärdas.

I tabell 4 presenteras de kontroller som vi har identifierat i processen för hantering av översättningstabellen mellan REX och Agresso samt en bedömning av huruvida kontrollerna är ändamålsenligt utformade.

Kontroll-nummer	Kontrollbeskrivning	Kontrollen är ändamålsenligt utformad	Kommentar
1	Automatiska felmeddelanden skickas för systemet i form av e-postmeddelande om fel uppstår i den månatliga överföringen mellan REX och Agresso.	Ej möjligt att utvärdera	Vid granskningen kunde vi inte ta del av något skickat felmeddelande eftersom det sällan uppstår fel i den månatliga överföringen mellan REX och Agresso och att loggar inte regelmässigt sparas
2	Endast godkända ändringar i tabellen genomförs.	Ja	Förändringar i tabellen genomförs som mindre förändringar enligt den process som beskrivs i stycket om programförändringar ovan, se kontroll 1, Tabell 1.

Tabell 4: Kontroller i processen för hantering av översättningstabellen mellan REX och Agresso

[9] Kontroll nr. 1 enligt *Tabell 4*.
[10] Kontroll nr. 2 enligt *Tabell 4*.

5. Iakttagelser och rekommendationer

I samband med granskningen identifierade vi ett antal förbättringsområden. Samtliga observationer och tillhörande rekommendationer har klassificerats utifrån följande skala:

Prioritet 1 - Risken bör hanteras snarast.
Prioritet 2 - Risken bör hanteras inom en snar framtid.
Prioritet 3 - Förbättringsområde som bör hanteras på sikt.

5.1 Inaktuella användare med höga behörigheter förekommer

Iakttagelse
I vår granskning noterade vi att SKV inte gör någon regelbunden granskning av användare med höga behörigheter, dvs. användare med åtkomst direkt till stordatormiljön genom behörighetsmodulen RACF. Det tillämpas inte heller någon process för upplägg eller borttag av sådana användare. Vidare noterade vi ett antal inaktiva konton med höga behörigheter.

Risk - prioritet 1
En avsaknad av regelbundna genomgångar av användare med höga behörigheter minskar möjligheten att upptäcka och åtgärda felaktigheter. Detta innebär i sin tur en ökad risk för obehörig åtkomst eller att användare av misstag eller uppsåtligen modifierar data i systemet utanför sina befogenheter.

Rekommendation
Vi rekommenderar KFM att ställa krav mot SKV, som sköter administrationen av höga behörigheter, att fastställa och införa rutiner för upplägg, borttag och regelbundna genomgångar av användare med höga behörigheter. Dessa rutiner bör utformas så att de säkerställer spårbarhet för att möjliggöra uppföljningar från KFM.

5.2 Regelbundna genomgångar av användare är inte ändamålsenligt utformade

Iakttagelse
Den genomgång av befintliga användare i REX som genomförs årligen utgår från personallistor och inte från användarlistor som dragits ut från systemet. Detta kan resultera i att genomgången inte inkluderar samtliga användare i REX då det exempelvis kan ligga kvar gamla användare som inte längre finns med på personallistorna. I vår granskning noterade vi att det förekom inaktuella användarkonton i vissa grupper i REX. Eftersom genomgången endast berör anställda på KFM inkluderas inte heller de användare i REX som lagts till från SKV. I granskningen noterade vi också att gruppen för behörighetsadministration på KFM även har möjlighet att lägga upp behörigheter till anställda på SKV trots att användare från SKV inte längre skall ha åtkomst till REX.

Risk - prioritet 2
Brister i regelbundna användargenomgångar kan resultera i att kvarliggande och inaktuella konton inte upptäcks eller att användare tilldelas högre behörigheter än vad

deras arbetsuppgifter kräver. Detta ökar risken för obehörig åtkomst eller att användare av misstag eller uppsåtligen modifierar data i systemet utanför sina befogenheter. Att gruppen för behörighetsadministration kan tilldela inte bara anställda på KFM behörigheter utan även anställda på SKV minskar kontrollen över behörigheterna vilket bidrar till ökad risk för bland annat obehörig åtkomst.

Rekommendation
Vi rekommenderar KFM att säkerställa att gruppen för behörighetsadministration på KFM inte har möjlighet att lägga upp behörigheter för anställda på SKV. Eftersom det i dagsläget inte är möjligt att på ett enkelt sätt dra ut listor med samtliga användare i REX, något som skulle möjliggöra ändamålsenliga genomgångar av användare, rekommenderar vi KFM att sammanställa en lista över de grupper av användare som har särskilda behörigheter eller som av andra skäl bedöms som särskilt viktiga att regelbundet kontrollera. Som ett komplement till de genomgångar som görs i dagsläget rekommenderar vi KFM att ta fram en rutin för regelbundna genomgångar av användarna på denna lista.

5.3 Test av programförändringar genomförs inte alltid

Iakttagelse
I vår granskning noterade vi att testrutinerna i programförändringsprocessen var bristfälliga på främst två punkter:

- Det finns inga krav från KFM:s sida som säkerställer att acceptanstester, dvs. tester som beställaren gör på den färdigutvecklade programförändringen, genomförs. SKV har därför inga fastställda rutiner för när och på vilket sätt KFM ska involveras för att genomföra acceptanstester. Detta medför att större förändringar inte alltid acceptanstestas och mindre förändringar aldrig acceptanstestas.
- Mindre programförändringar testas endast vid de tillfällen då utvecklaren bedömer det nödvändigt och denna bedömning varken kontrolleras eller dokumenteras.

Risk - Prioritet 2
Bristfälliga testrutiner ökar risken för driftsättning av otillfredsställande eller felaktiga programförändringar vilket kan äventyra systemets produktionsmiljö och orsaka oväntade avbrott i verksamheten.

Rekommendation
Vi rekommenderar KFM att ställa krav på SKV, som hanterar alla programförändringar, att tydliggöra när tester bör genomföras på förändringar av mindre program-förändringar samt dokumentera och kommunicera detta till samtliga berörda utvecklare. Vidare rekommenderar vi KFM att se över den dokumenterade processen för förändringshantering som KFM delar med SKV och säkerställa att rutiner finns för acceptanstester för alla typer av förändringar.

5.4 Avsaknad av specifikation kring säkerhetskopiering och återläsningstester

Iakttagelse
I KFM:s interna styrdokument finns riktlinjer kring hur säkerhetskopiering och återläsningstester ska hanteras. I granskningen noterade vi dock att inga specifika krav gällande detta finns dokumenterade i det serviceavtal som KFM har med SKV.

Risk - prioritet 2
Bristande rutiner kring säkerhetskopiering och återläsningstester kan resultera i förlust av för verksamheten viktig information. Avsaknad av formell kravspecifikation i avtalet med driftleverantören ökar risken för att överenskomna rutiner inte efterlevs.

Rekommendation
Vi rekommenderar KFM att se över de brister som avtalet med SKV har och säkerställa att de åtgärdas i den upphandling som nu pågår av driftleverantör. Avtalet bör bl.a. specificera:

- Vilka delar av systemet som omfattas av rutinerna för säkerhetskopiering
- Med vilken frekvens säkerhetskopiering ska göras
- Hur säkerhetskopiorna ska förvaras
- Hur länge säkerhetskopiorna ska förvaras
- Med vilken frekvens återläsningstester ska göras

5.5 Begränsad spårbarhet i processen för behörighetshantering

Iakttagelse
I vår granskning noterade vi svårigheter med att hitta beställningsunderlag för flertalet användare i REX. Detta gör det svårt att bekräfta att rutinerna som finns för upplägg och ändring av användare efterlevs. En förklaring till denna begränsade spårbarhet är emellertid att rutinen för arkivering av beställningsblanketter infördes i slutet av 2011 och därmed är relativt ny. Tidigare har blanketterna arkiverats av respektive personalchef men den nya rutinen innebär att en behörighetssamordnare hanterar arkiveringen centralt. Vid granskningstillfället bekräftade vi att arbete pågår med att samla in blanketterna från personalcheferna för central arkivering.

Risk - prioritet 3
Bristande spårbarhet i behörighetshanteringen som till stor del kontrolleras genom manuella kontroller ökar risken för att kontrollerna inte utförs enligt beskrivning. Detta kan leda till att felaktiga behörigheter läggs upp. Bristande spårbarhet kan också försvåra arbetet med att upptäcka felaktigheter i processen och härleda dessa till rätt grundorsak.

Rekommendation
Vi rekommenderar KFM att fortsätta arbetet med insamlandet av beställnings-blanketter för att säkerställa att processen går att spåra.

Bilaga A Respondenter och granskade dokument

Respondenter

Befattning
Anställda inom verksamhetsutveckling
Behörighetsadministrator REX
Behörighetssamordnare REX
Informationssäkerhetschef
Informationsägare REX
Systemadministrator REX
Säkerhetschef
Uppdragsledare REX
Utvecklare REX

Granskade dokument

Titel	Datum
10.1_Driftsrutiner_driftansvar 120116.pdf	2012-01-16
10.5_Sakerhetskopiering 120116.pdf	2012-01-16
Applikationsdrift 2012.doc	2012 version 2.0
Beslut om införande av Behörighetsforum	2012-10-11
Beslut om indelning av särskilda behörigheter.pdf	2012-08-31
Bilaga x Specifikation servicetider m.m. 2012.doc	2012-02-07
Instruktioner årlig behörighetsgenomgång121001.pdf	2012-10-01
IT-avdelningens rekommendation av driftsättning.pdf	2012-11-07
Lathund behörighetsrutin.pdf	-
Månadsrapport - från Skatteverket till KFM.pdf	2012-11-19
Omfattningsbeskrivning.pdf	2011-10-31
Statuskontroll D-CAB.pdf	2012-11-06
Testrapport systemintegrationstest.pdf	2012-10-12
Testrapport.pdf	2012-11-28
Utvecklingsplan Verkställighet och Summarisk process s 21-24.pdf	2011-04-04