DNR: 32-2012-0554

KRONOFOGDEMYNDIGHETEN
172 21 SUNDBYBERG

BESLUT: 2013-03-18

Revision av den interna kontrollen kring uppbördssystemet REX

1 Inledning

Riksrevisionen har som ett led i den årliga revisionen 2012 av Kronofogdemyndigheten (KFM) granskat den interna kontrollen kring uppbördssystemet REX.

Granskningen har omfattat en kartläggning av KFM:s processer för programförändringar, behörighetshantering och driftsrutiner för systemet REX, samt identifiering och testning av kontroller i dessa system. Kartläggningen innefattar även kontroller för att säkerställa att inga förändringar sker i överföringen av information från REX till huvudboken i ekonomisystemet Agresso. Iakttagelser och förbättring.

I granskningen har Riksrevisionen biträtts av Ernst & Young AB (E&Y). Granskningen har resulterat i iakttagelser vilka Riksrevisionen vill fästa Kronofogdemyndighetens uppmärksamhet på i denna revisionsrapport.

Riksrevisionen önskar information senast 2013-05-01 med anledning av iakttagelserna i rapporten.

Som framgår av Ernst & Youngs granskning (bilaga 1) bedöms KFM i flera avseenden, ha ändamålsenligt utformade kontroller men att det i vissa avseenden finns utrymme för förbättring.

Innehållsförteckning

DNR: 32-2012-0554

KRONOFOGDEMYNDIGHETEN
172 21 SUNDBYBERG

BESLUT: 2013-03-18

2 Iakttagelser och rekommendationer

Nedan redovisas översiktligt de iakttagelser som noterats. I bilaga 1 sker en fördjupad redovisning. Iakttagelserna nedan klassificeras utifrån:

- Prioritet 1 – risken bör hanteras snarast
- Prioritet 2 – risken bör hanteras inom snar framtid
- Prioritet 3 – förbättringsområde som bör hanteras på sikt

2.1 Prioritet 1 – risken bör hanteras snarast

2.1.1 Inaktuella användare med höga behörigheter förekommer

Iakttagelse

Det görs inte någon regelbunden genomgång 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 noterades 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. Innebär en ökad risk för obehörig åtkomst eller att användare av misstag eller uppsåtligen modifierar data i systemet utanför sina befogenheter.

Rekommendation

KFM rekommenderas ställa krav mot Skatteverket (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.

DNR: 32-2012-0554

KRONOFOGDEMYNDIGHETEN
172 21 SUNDBYBERG

BESLUT: 2013-03-18

2.2 Prioritet 2 – risken bör hanteras inom snar framtid

2.2.1 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 granskningen noterades att det förekom inaktuella användarkonton avseende 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 noterades 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

KFM rekommenderas 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, rekommenderas 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 rekommenderas KFM att ta fram en rutin för regelbundna genomgångar av användarna på denna lista.

2.2.2 Test av programförändringar genomförs inte alltid

Iakttagelse

I granskningen noterades 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 kontrolleras eller dokumenteras inte.

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

KFM rekommenderas att ställa krav på SKV, som hanterar alla programförändringar, att tydliggöra när tester bör genomföras på förändringar av mindre programförändringar samt dokumentera och kommunicera detta till samtliga berörda utvecklare. Vidare rekommenderas 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.

2.2.3 Avsaknad av specifikation kring säkerhetskopiering och återläsningstester

Iakttagelse

I KFM:s interna styrdokument finns riktlinjer kring hur säkerhetskopiering och återläsningstester ska hanteras. I granskningen noterades 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

KFM rekommenderas att se över de brister som avtalet med SKV har och säkerställa att de åtgärdas i den upphandling som nu, enligt uppgift, 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

2.3 Prioritet 3 – förbättringsområde som bör hanteras på sikt

2.3.1 Begränsad spårbarhet i processen för behörighetshantering

Iakttagelse

I granskningen noterades 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 bekräftades 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

KFM rekommenderas att fortsätta arbetet med insamlandet av beställningsblanketter för att säkerställa att processen går att spåra.

DNR: 32-2012-0554

KRONOFOGDEMYNDIGHETEN
172 21 SUNDBYBERG

BESLUT: 2013-03-18

Ansvarig revisor Lars Nordstrand har beslutat i detta ärende. Revisionsledare Emma Karlemo har varit föredragande.

Lars Nordstrand Emma Karlemo

Bilaga 1 Ernst & Young AB, Granskning med fokus på IT – risker, Kronofogdemyndigheten

Kopia för kännedom:

Regeringen
Finansdepartementet
Finansdepartementet, budgetavdelningen