DNR: 32-2013-0456

SKATTEVERKET
171 94 SOLNA

BESLUT: 2014-05-19

IT-generella kontroller i Agresso, skattekontosystemet, Moms AG och Tina

Riksrevisionen har som ett led i den årliga revisionen av Skatteverket granskat IT-generella kontroller i ekonomisystemet Agresso, skattekontosystemet samt debiteringssystemen för moms och arbetsgivaravgifter (Moms AG) och inkomstskatt (Tina).

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa Skatteverkets uppmärksamhet på i denna revisionsrapport. Riksrevisionen önskar information senast 2014-06-19 med anledning av våra iakttagelser i denna rapport.

Revisionsrapporten innehåller uppgifter som omfattas av sekretess enligt 18 kap. 8 och 13 §§ Offentlighets- och sekretesslagen (2009:400), varför det finns en hemlig och en öppen version av rapporten. Detta är den öppna versionen. Den icke öppna versionen finns i en hemlig bilaga 1.

Sammanfattning

Skatteverket har en komplex IT-miljö med IT-system som är väsentliga för såväl den finansiella redovisningen och resultatredovisningen som för verksamhetens fortlöpande drift. Med anledning av detta är det viktigt att det finns en god intern kontroll i Skatteverkets rutiner kring IT-systemen.

Riksrevisionen konstaterar att Skatteverket behöver formalisera och förbättra rutinerna för hantering av programförändringar och behörigheter i ekonomisystemet Agresso. Därtill behöver Skatteverket införa uppföljning av åtkomsten som utvecklingspersonal har till IT-systemens produktionsmiljöer för att minska risken för att otillåtna ändringar utförs. Skatteverket behöver även stärka rutinerna vid tilldelning och uppföljning av höga behörigheter i operativsystem. Slutligen konstaterar Riksrevisionen att det finns vissa brister i Skatteverkets rutiner för hantering av backup och lagring av information.

1. Bristande rutiner för hantering av behörigheter och programförändringar i Agresso

Agresso är Skatteverkets ekonomisystem och är därmed väsentligt för den finansiella rapporteringen som Skatteverket lämnar i sin årsredovisning. Riksrevisionen har vid flera tillfällen

påtalat att det finns brister i Skatteverkets rutiner för hantering av behörigheter och programförändringar i Agresso.[1] Bristerna kvarstår även 2013.

1.1 Behörigheter

Skatteverkets administration av behörigheter i Agresso hanteras utanför Skatteverkets gemensamma behörighetskontrollsystem. I princip alla Skatteverkets anställda använder Agresso för tidrapporter, attestering av leverantörsfakturor och annan administration via ett webbgränssnitt. Dessa behörigheter tilldelas när personerna anställs. Därutöver finns anställda på Statens Servicecenter, Ekonomiavdelningen och systemförvaltningen (A3S) som har högre behörigheter i Agresso i en klientversion som installeras på den anställdes dator. Totalt finns cirka 30 olika rollbaserade behörigheter i Agresso, varav vissa är mer känsliga och innebär högre rättigheter i systemet.

Det saknas en rutinbeskrivning för behörigheter i Agresso

Det finns en formell riktlinje för behörigheter, daterad 2013-11-11. Det finns även en separat rutin för hantering av behörigheter i Agresso för användare på Statens Servicecenter. Det saknas dock en rutinbeskrivning för administration av behörigheter i Agresso för Skatteverkets anställda på Ekonomiavdelningen och A3S. Avsaknaden av dokumenterade rutiner ökar risken för att behörigheter hanteras felaktigt, vilket i sin tur kan leda till att obehöriga får åtkomst till systemet eller att information ändras på ett felaktigt sätt. Dokumenterade rutiner minskar även risken för personberoenden i olika arbetsmoment.

Tilldelning av höga systembehörigheter har gjorts utan dokumenterade godkännanden

Tilldelning av högre behörigheter i Agresso ska göras först efter godkännande från respektive medarbetares chef, via epost eller särskild blankett.[2] Riksrevisionens granskning visar dock att Skatteverket har tilldelat medarbetare höga behörigheter utan sådana formella godkännanden. Enligt uppgift har muntligt godkännande lämnats för dessa individer, men det finns ingen dokumentation på Skatteverket som verifierar detta.[3] Utan dokumenterade godkännanden av nya behörigheter saknas det dokumentation som stödjer behörigheternas giltighet och det finns därmed inte en tillfredsställande intern styrning och kontroll i behörighetshanteringen.

Rekommendation

Skatteverket rekommenderas att införa rutiner som säkerställer att det alltid finns skriftliga godkännanden vid tilldelning, ändring och borttag av behörigheter i Agresso. En formell och

[1] Senast i revisionsrapport *Skatteverkets årsredovisning 2012 samt granskning av uppbördsprocesser* 2013-05-02, dnr 32-2012-0555, men även i Revisions-PM *Skatteverket – Generella IT-kontroller i Agresso och Palasso* 2010-05-26, dnr 32-2009-0512.
[2] Blankett används på Statens Servicecenter och epost används för Skatteverkets anställda.
[3] Iakttagelsen avser två användare. Behörigheterna har inaktiverats under 2013 till följd av att individerna har slutat.

uppdaterad rutinbeskrivning bör upprättas och beslutas för anställda på Skatteverket, för att minska risken för felaktig administration av behörigheter.

Skatteverket rekommenderas vidare att se över möjligheten att inkludera Agresso i den nya gemensamma applikationen för behörighetsadministration.

1.2 Programförändringar

Det saknas en dokumenterad rutin för hantering av programförändringar i Agresso
Skatteverket saknar en aktuell och formaliserad rutin för systemändringar i Agresso. Det finns dokumenterade rutiner som inte följs eftersom de enligt uppgift är föråldrade. Avsaknaden av formaliserade rutiner ökar risken för att ändringar i Agresso inte hanteras korrekt. Det försvårar också möjligheten för Skatteverket att följa en förändring genom processen samt ökar risken för att förändringar som inte är godkända driftsätts.

Avsaknad av dokumenterade beslut vid systemändringar i Agresso
Riksrevisionens granskning visar att de funktionalitetsförändringar som har gjorts i Agresso under 2013 inte har föregåtts av dokumenterade beslut eller beställningsunderlag. Det finns inget skriftligt beslut om att systemändringarna ska genomföras och inte heller någon dokumentation om att ändringarna kan produktionssättas efter genomförda tester. Enligt uppgift tas samtliga beslut muntligen. Avsaknaden av rutiner som innehåller krav på dokumentation ökar risken för att ändringar genomförs som inte är förankrade i organisationen, eller att systemet inte fungerar i enlighet med uppsatta krav och mål. Därtill ökar risken för driftstörningar, till exempel som följd av att förändringarna inte har testats färdigt eller att de krockar med andra aktiviteter. Dessa risker minskar genom införande av dokumenterade beslut och godkännanden i samband med program-förändringar.

Testdokumentation saknas
Det saknas testdokumentation för den systemändring i Agresso som följde av Skatteverkets byte till Windows 7.

Rekommendation
Skatteverket rekommenderas att utveckla och besluta om en rutin för förändringshantering i Agresso. Rutinen bör omfatta kravställning, godkännande, ändring, test och produktionssättning av förändringar. Alla ändringar bör föregås av ett formellt beslut att genomföra förändringen samt ett formellt beslut inför produktionssättning för att säkerställa att nödvändiga tester är genomförda och att verksamheten är redo för införandet. Besluten bör tas av systemägare eller motsvarande roll med huvudansvar för Agresso. Rutinen bör även inkludera krav på loggning och spårning samt innehålla rutiner för till exempel prioritering och akuta förändringar.

Rutinen bör helst vara kopplad till ett ärendehanteringsverktyg där det är möjligt att följa en förändring genom stegen önskemål, beslut, godkännande av kravspecifikation, testprotokoll, godkända tester, prioritering vid införande, plan för återställning av miljö före senaste ändring (rollback), beslut om införande samt dokumenterad återkoppling med information om produktionssättning.

Slutligen rekommenderas Skatteverket att säkerställa att genomförda tester dokumenteras med hjälp av ett testprotokoll eller liknande dokument. Detta gäller även systemändringar där färdiga testprotokoll inte tillhandahålls av leverantören till systemet.

2. Utvecklare med tillgång till produktionsmiljö

Eftersom stora delar av Skatteverkets IT-system är egenutvecklade har Skatteverket egen utvecklingspersonal. Riksrevisionen har noterat att det finns utvecklare som har administrationsbehörigheter i produktionsmiljöerna för skattekontot, Moms AG och Tina.

Riksrevisionen har tidigare påtalat denna brist för Skatteverket.[4] Skatteverket har då uppgett att det pågår ett arbete med att införa en rutin för att följa upp utvecklares åtkomst till produktionsmiljöer. Efter årets granskning kan vi konstatera att så inte är fallet.

Rekommendation

Skatteverket rekommenderas att begränsa antalet utvecklare med tillgång till produktionsmiljöer i den utsträckning det går, utan att verksamheten påverkas negativt. Om Skatteverket bedömer att det fortsatt finns utvecklare som behöver ha sådan behörighet rekommenderas Skatteverket att införa kontroller och uppföljning för att hantera risker som detta medför.

Rekommendationerna ovan gäller även system som inte har ingått i Riksrevisionens granskning men där motsvarande problematik finns. Utvecklares tillgång till produktionsmiljöer är en risk som Skatteverket löpande behöver bevaka, värdera och följa upp.

3. Brister i uppföljning och tilldelning av behörigheter

3.1 Bristande uppföljning av applikationsbehörigheter

Varje år före den 31 december ska Skatteverkets chefer bekräfta behörigheter för sina medarbetare för att dessa ska fortsätta gälla. Som en följd av att ett nytt behörighetskontrollsystem var planerat att införas våren 2013 gjordes inte denna genomgång inför 2012-12-31. Införandet av behörighetskontrollsystemet blev sedan försenat och genomfördes inte förrän i november 2013. Detta medförde att det när Riksrevisionens granskning genomfördes inte hade gjorts någon uppföljning av lämpligheten i befintliga behörigheter sedan 2011-12-31. Enligt uppgift var nästa

[4] Revisionsrapport *Skatteverkets årsredovisning 2012 samt granskning av uppbördsprocesser* 2013-05-02, dnr 32-2012-0555 och revisionsrapport *Revision av uppbördsprocessen Moms* 2012-02-03, dnr 32-2011-0544.

uppföljning av behörigheterna planerad till slutet av mars 2014. Som ett resultat av detta hade behörigheternas lämplighet, vid utgången av 2013, inte bekräftats på över två år. Iakttagelsen avser behörigheter som hanteras inom behörighetskontrollsystemet. Även för Agresso har dock brister i uppföljningen av befintliga behörigheter noterats. Riksrevisionen har vid granskningen inte kunnat verifiera att Skatteverket genomför uppföljningar av applikationsbehörigheter i Agresso.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att snarast genomföra uppföljning av befintliga applikationsbehörigheter i Skatteverkets system, om sådan ännu inte har gjorts. Därtill rekommenderas Skatteverket att göra sådan uppföljning minst årligen framöver.

3.2 Tilldelning av höga behörigheter i operativsystem

Skattekontosystemet, Moms AG, Tina och den klientbaserade delen av Agresso hanteras av operativsystemet Unix. Inloggningen till Skatteverkets nätverk och den webbaserade delen av Agresso hanteras av operativsystemet Windows. Riksrevisionen har granskat tilldelning och uppföljning av priviligierade behörigheter som finns i dessa operativsystem. Behörigheterna i Unix hanteras inom Skatteverkets gemensamma behörighetskontrollsystem medan Windows hanteras utanför denna rutin. Detta får till följd att behörigheterna i Unix vid granskningens tillfälle inte hade omfattats av någon periodisk genomgång sedan 2011-12-31. För behörigheterna till Windows har Riksrevisionen uppmärksammat att det inte görs någon periodisk genomgång alls.

Rekommendation

Skatteverket rekommenderas att införa rutiner för periodisk genomgång av priviligierade behörigheter i operativsystemet Windows. Därtill rekommenderas Skatteverket att stärka upp rutinerna för tilldelning av behörigheter i operativsystem och säkerställa att det alltid finns dokumenterade beslut.

4. Vissa brister i programförändringsrutiner för skattekontot och Moms AG

4.1 Avsaknad av dokumenterade tester i skattekontosystemet och Moms AG

Skatteverkets rutin för förändringshantering i skattekontot innehåller inte några krav på formell dokumentation av tester. Även om tester utförs finns det således inte nödvändigtvis dokumentation från dessa. För de programförändringar som har ingått i Riksrevisionens granskning 2013 har det inte funnits någon dokumentation.

Rekommendation
Riksrevisionen rekommenderar Skatteverket att införa rutiner som säkerställer att tester som genomförs av planerade programförändringar i skattekontot och i Moms AG dokumenteras. Detta kan enklast göras genom standardiserade testprotokoll eller dylika dokument.

4.2. Programförändringsrutinen för Moms AG innehåller inte krav på att verksamhetens krav och godkännande ska dokumenteras

Riksrevisionens granskning av ett urval av programförändringar i Moms AG under 2013 visar att det inte finns en fastställd kravspecifikation eller liknande överenskommelse om vilka av verksamhetens krav som ingår i respektive release eller produktionssättning av Moms AG. Skatteverkets rutin för programförändringar i Moms AG innehåller inte heller tydliga krav på att sådan kravspecifikation ska upprättas och godkännas. När fastställande och godkännande av verksamhetens krav inte dokumenteras på ett tydligt sätt försämras spårbarheten i genomförda förändringar. Detta medför att det kan finnas osäkerhet kring vilka krav eller önskemål som har beslutat att införas, eller oklarheter kring vilken version av kravdokument som har driftsatts.

Rekommendation
Skatteverket rekommenderas att komplettera den befintliga programförändringsrutinen för Moms AG med krav på att formell dokumentation av fastställande och godkännande av kravdokument ska upprättas för varje programförändring.

5. Brister i IT-driftrutiner

5.1 Brister i hantering av backup och lagring

Skatteverket har en intern leveransbeskrivning som övergripande anger omfattningen på backup och lagring. Det finns även driftdokumentation med arbetsbeskrivningar för hur backup och lagring genomförs. En brist som Riksrevisionen har noterat är dock att det inte finns kravställning från verksamheten rörande omfattningen på backup och lagring på applikationsnivå. Detta ökar risken för att backupdata inte finns tillgänglig i tillräcklig utsträckning, alternativt att alltför mycket resurser läggs på detta ändamål. Det ökar även risken att gällande lagar och förordningar avseende lagring inte följs.

Rekommendation
Skatteverket rekommenderas att införa rutiner som innebär att verksamheten definierar krav på backup och lagring per applikation.

SKATTEVERKET
171 94 SOLNA

5.2 Återläsningstester görs inte av backuper

Skatteverket har inte rutiner eller riktlinjer som definierar i vilken utsträckning återläsningstester av backuper ska genomföras. Det finns inte heller någon formell kravställning från verksamheten för återläsning på applikationsnivå. Dessa brister är generella och inte specifika för de system som har ingått i Riksrevisionens granskning. För de system som har ingått i granskningen kan vi konstatera att det inte har genomförts några återläsningstester under 2013 för att verifiera att backuper fungerar. Att återläsningstester inte görs regelbundet liksom att krav inte finns på detta från verksamheten ökar risken för att återläsning av data inte uppfyller önskade nivåer alternativt att alltför mycket resurser nyttjas för detta ändamål. Därtill ökar risken för att verksamhetskritisk data inte kan återläsas i händelse av systemkrasch eller vid andra behov av att återskapa tidigare versioner av data.

Rekommendation

Skatteverket rekommenderas att vidta följande åtgärder rörande återläsning av backuper:

- Att ta fram generella riktlinjer för rutinmässiga återläsningstester.
- Att verksamhetsansvariga tar fram krav på behov av återläsningstester per applikation.
- Att gruppen för data och lagring och backup genomför återläsningstester i enlighet med riktlinjer och krav från verksamheten.

Ansvarig revisor Lars Nordstrand har beslutat i detta ärende. Uppdragsledare Ulrika Meyer har varit föredragande

Lars Nordstrand Ulrika Meyer

Kopia för kännedom:

Regeringen
Finansdepartementet
Finansdepartementet, budgetavdelningen