RIKSREVISIONEN

SKATTEVERKET
171 94 SOLNA

DNR: 3.1.2-2016-0617
BESLUT: 2017-03-10

Granskning av generella IT-kontroller för ett urval system vid Skatteverket

Som ett led i granskningen av årsredovisningen med syfte att göra uttalanden om denna har Riksrevisionen även granskat rutiner och kontroller inom IT. Denna granskning syftar till att verifiera hur Skatteverket säkerställer en säker hantering av behörigheter till IT-system samt införande av förändringar i IT-system. Bakgrunden är att dessa kontroller bedöms vara viktiga för att säkerställa en fullständig och korrekt årsredovisning. Riksrevisionen har därför granskat ett urval av myndighetens centrala IT-system. Granskningen har omfattat systemet för skattekontot, systemen Kuling, Moms AG och Tina samt beräkningsmodulerna BD1000 och BD2000.

Riksrevisionen har utfört en kartläggning och testning av generella IT-kontroller för ovan uppräknade IT-system. Granskningen har i första hand omfattat Skatteverkets rutiner och kontroller för systemförändringar och behörighetshantering.

De punkter som är upptagna i denna revisionsrapport är sådana som Riksrevisionen vill fästa ledningens uppmärksamhet på. Iakttagelserna avser endast rutiner och kontroller för de system och rutiner som har granskats, men eftersom granskningen gäller generella IT-kontroller kan iakttagelserna och rekommendationerna vara aktuella att beakta även för andra system inom Skatteverket.

Riksrevisionen önskar information senast 2017-04-10 med anledning av våra iakttagelser i denna rapport.

Sammanfattning

Skatteverket har en mycket omfattande och komplex IT-miljö med IT-system som är väsentliga för såväl finansiell redovisning och resultatredovisning, som för verksamhetens fortlöpande drift. Det är därför viktigt att det finns god intern kontroll i samtliga rutiner kring Skatteverkets verksamhetskritiska IT-system.

Riksrevisionen bedömer att det finns behov av att förbättra Skatteverkets rutiner för tilldelning och användning av de högst priviligierade IT-behörigheterna för myndighetens verksamhetskritiska IT-system.

Riksrevisionen bedömer även att Skatteverket bör verka för att rutiner för programförändringar är enhetliga och tillämpas med god intern kontroll för samtliga

verksamhetskritiska IT-system samt att om möjligt separera åtkomst till utvecklings- och produktionsmiljö.

1. Brister i hanteringen av behörigheter och rättigheter

1.1 Ett stort antal användare med höga priviligierade IT-behörigheter

Riksrevisionens granskning har visat att ett stort antal personer tillhör en hög behörighetsklass. För att erhålla de rättigheter som denna behörighetsklass medger krävs dock även att användaren har ett användarkonto till aktuell server. De höga behörigheter som denna behörighetsklass innebär, ger möjlighet att påverka systemen där påverkan dessutom kan vara svår att spåra.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att bedöma behovet av denna höga behörighetsklass. Skatteverket bör överväga att ta bort behörighetsklassen alternativt att minska omfattningen av den. I det fall Skatteverket väljer att fortsätta med behörighetsklassen bör Skatteverket kontinuerligt granska de loggar som förs över användningen av höga behörigheter i verksamhetskritiska system.

1.2 Avsaknad av en formaliserad rutin för tilldelning av domänadministratör

I Skatteverkets Windowsbaserade nätverk används Active Directory för hantering av åtkomst. Den högsta behörigheten i Active Directory benämns domänadministratör. Denna roll innebär bland annat att man i princip kan tilldela godtyckliga personer (inklusive sig själv) godtycklig behörighet i verksamhetens system.

Granskningen har visat att rättigheterna som domänadministratör tilldelas informellt, detta då Skatteverket inte har någon formellt dokumenterad rutin för tilldelning av domänadministratörsrättigheter. Granskningen visar också att Skatteverket inte dokumenterar tilldelningen av dessa domänadministratörsrättigheter.

Informell tilldelning av domänadministratörer ökar risken för att rättigheten tilldelas fler användare än nödvändigt och att tilldelningen inte sker baserat på behovet utifrån individens arbetsuppgifter och ansvar.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att dokumentera rutinen för tilldelning av rättigheten domänadministratör. Riksrevisionen rekommenderar även Skatteverket att tillse att sådana tilldelningar dokumenteras.

1.3 Skatteverkets Active Directory har ett flertal domänadministratörer

Riksrevisionens granskning har visat att Skatteverket för närvarande har ett flertal domänadministratörer i sitt Active Directory. Riksrevisionen har i granskningen inte kunnat se att Skatteverket följer upp loggar avseende åtgärder utförda av domänadministratörerna.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att bedöma behovet av antalet domänadministratörer. Ambitionen bör vara att så långt som möjligt minska antalet domänadministratörer på grund av deras långtgående rättigheter. Riksrevisionen rekommenderar också att Skatteverket kontinuerligt följer upp loggarna över domänadministratörernas åtgärder.

2. Brister i rutiner för programförändringar

2.1 Myndighetsgemensam rutin för programförändringar är inte känd inom myndigheten

Riksrevisionen har under granskningen noterat att det finns framtagna riktlinjer för Skatteverkets processer för IT-leverans som på en övergripande nivå beskriver mål och principer för processen att hantera systemförändringar. Därutöver finns det detaljerade processbeskrivningar inom tjänsteleveransprocesserna för förändringshantering samt framtagna riktlinjer och metodbeskrivningar för test och diverse lathundar och detaljerade kravchecklistor. Granskningen har dock visat att befintliga gemensamma rutiner för programförändringar inte är kända inom myndigheten och tillämpas därmed inte för de olika systemen på Skatteverket. Däremot har Riksrevisionen noterat att det finns enskilda rutiner framtagna för vissa av de specifika system som varit föremål för denna IT-revision, men inte för alla.

Avsaknad av kunskap och kännedom om en myndighetsgemensam rutin för programförändringar medför att det utformas enskilda rutiner för varje system eller att det saknas rutiner samt att arbetssättet inom myndigheten inte blir enhetligt.

Granskningen har även visat att underlag för formella godkända beställningar av programförändringar i vissa fall saknas och att kvaliteten på testdokumentationen varierar beroende på system och att den dokumenteras i olika verktyg.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att föra ut information och öka kunskapen om vilket stöd inom förändringshantering som finns framtaget centralt både vad gäller riktlinjer och processer men även i form av verktyg för ärendehantering och tester samt påtala vikten av att dessa riktlinjer och processer ska efterlevas inom myndigheten. Därutöver bör en process för att följa upp efterlevnad av interna rutiner och processer utformas och implementeras.

2.2 Avsaknad av dokumenterade tester för BD1000 och BD2000

Riksrevisionens granskning har inkluderat de två beräkningsmodulerna BD1000 och BD2000. De två modulerna är centrala vid beräkningar av skatt för fysiska respektive juridiska personer. Granskningen har visat att hantering av programförändringar för beräkningsmodulerna BD1000 och BD2000 är informella och att utförda tester och godkännande inte dokumenteras.

Avsaknad av formella godkännanden och dokumentation av utförda tester medför sämre spårbarhet och ökar risken för felaktiga förändringar i produktionsmiljön

Rekommendation

Riksrevisionen rekommenderar Skatteverket att programförändringar för BD1000 och BD2000 hanteras enligt Skatteverkets generella riktlinjer för programförändringar och i enhetlighet med ovan av Riksrevisionen rekommenderade myndighetsgemensamma rutin för systemförändringar.

2.3 Utvecklare har åtkomst till produktionsdatabaser

Riksrevisionen har under årets granskning, liksom tidigare år, noterat att för de två handläggningssystemen TINA och Kuling har flera av utvecklarna skrivrättighet till och kan därmed göra ändringar i systemens produktionsdatabas. Vidare noterades att alla utvecklare har möjlighet att ta sig rättigheter för att få åtkomst till produktionsmiljön och att ingen systematisk uppföljning av detta sker. Därutöver uppmärksammade Skatteverket i samband med vår granskning att flertalet behörigheter till TINA var inaktuella och kunde tas bort.

Att inte separera åtkomst mellan utvecklings- och produktionsmiljöer i programändringsflödet medför att en enskild individ på egen hand kan genomföra en programförändring utan att beslutade kontroller har genomförts. Detta ökar risken för produktionssättning av såväl avsiktliga som oavsiktliga fel i systemen.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att, om det är praktiskt möjligt, tillse att separerade arbetsuppgifter upprätthålls genom att utvecklare inte också har skrivrättigheter till produktionsdatabasen. Om detta inte fullt ut är praktiskt genomförbart bör en manuell kontroll upprättas där Skatteverket implementerar en generell rutin för uppföljning av utvecklares åtkomst till produktionsmiljöer på alla relevanta system.

Ansvarig revisor Charlotte Ehrengren har beslutat i detta ärende. Granskningsledare Louise Ros har varit föredragande.

Charlotte Ehrengren Louise Ros

Kopia för kännedom:

Regeringen
Finansdepartementet
Finansdepartementet, budgetavdelningen