RIKSREVISIONEN

SKATTEVERKET
171 94 SOLNA

DNR: 3.1.2-2017-0640
BESLUT: 2018-02-26

Granskning av generella IT-kontroller för ett urval system vid Skatteverket 2017

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. Riksrevisionen granskade detta även under 2016. Iakttagelserna från den granskningen avrapporterades till Skatteverket (dnr 3.1.2-2016-0617).

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 2018-03-28 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 användares åtkomst till utvecklings- och produktionsmiljö. Riksrevisionen vill slutligen göra Skatteverkets ledning uppmärksam på att säkerhetskopior av verksamhetskritisk data inte förvaras geografiskt åtskild från produktionsdata.

1. Brister i hanteringen av behörigheter och rättigheter

1.1 Ett stort antal användare har fortsatt höga priviligierade IT-behörigheter

Riksrevisionens granskning har i år, likt föregående år, 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 så kallat smartkort för att få återkomst till aktuell server. De höga behörigheter som denna behörighetsklass innebär, ger användaren möjlighet att påverka systemen, där påverkan dessutom kan vara svår att spåra. Många användare med höga behörigheter kan innebära ökad risk för obehörig åtkomst till program och information. Vidare kan detta öka risken för felaktigheter och misstag på grund av okunskap, slarv eller oegentligheter. Riksrevisionen är medveten om att Skatteverket har påbörjat ett arbete för att åtgärda detta men vid årets granskning kvarstår dock iakttagelsen.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att fortsätta sitt arbete att begränsa antalet användare med denna höga behörighetsklass.

1.2 Skatteverkets Active Directory har fortsatt ett flertal domänadministratörer

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. Riksrevisionens granskning har visat att Skatteverket även i år har ett flertal domänadministratörer i sitt Active Directory.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att bedöma behovet av antalet domänadministratörer. Ambitionen bör vara att så långt som möjligt minimera antalet domänadministratörer på grund av deras långtgående rättigheter, detta kan kombineras med att dessa rättigheter endast tilldelas under begränsad tid och vid behov.

1.3 Åtkomst till systemresurser loggas men följs inte upp regelbundet

Skatteverket har en utförlig loggning av aktiviteter i applikationer och databaser. Bland annat så loggas aktiviteter för ovan nämnda höga behörigheter och domänadministratörer för Active Directory. Dessa loggar lagras under en längre tidsperiod, på ett vad Riksrevisionen förstår systematiskt och strukturerat sätt. Det utförs dock ingen systematisk granskning och uppföljning av dessa loggar. Avsaknad av strukturerad granskning och uppföljning av loggar innebär en risk att Skatteverket trots loggning inte upptäcker olämpliga aktiviteter.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att kontinuerligt följa upp och granska de loggar som förs över användningen av ovan nämnda höga behörigheter i verksamhetskritiska system och av Active Directory domänadministratörer. Riksrevisionen har noterat att uppbyggnad av en funktion för granskning av loggar från verksamhetskritiska system initierats (SOC), men att arbetet och dess implementering ännu inte är färdigt. Riksrevisionen rekommenderar Skatteverket att fullfölja arbetet.

2. Brister i rutiner för programförändringar

2.1 Brister i enhetlighet vid programförändringar samt otydlig spårbarhet vid förändringar i Skattekontot

Skatteverket har ett antal olika rutiner och styrande dokument som beskriver hur myndigheten skall arbeta med programförändringar. Granskningen har dock visat att utförandet av programförändringar skiljer sig åt baserat på hur förändringsbehovet uppstår, exempelvis om det är fråga om så kallad nyutveckling, vidareutveckling eller vidmakthållande. Dessutom har vi även i årets granskning noterat att tillämpningen av de styrande dokumenten gällande programförändringar skiljer sig åt mellan olika applikationer.

Vi har i samband med årets granskning noterat att det för applikationen Skattekontot är svårt att följa kedjan från beställning av programförändring från verksamheten till acceptanstest av beställd funktionalitet och produktionsgodkänd programförändring. En orsak till att det är svårt att följa är att acceptanstester dokumenteras på olika sätt beroende på vem som utför testerna. En annan orsak är att kopplingen mellan den beställda programförändringen, de utförda acceptanstesterna och godkännandet för produktionssättning inte är tydlig. Avsaknad av tydlig koppling mellan beställd programförändring, acceptanstest och godkännande för produktionssättning innebär att det är svårt att verifiera att beställd funktionalitet fungerar som avsett, samt att samtliga produktionssatta programförändringar är godkända av verksamheten. Det innebär i sin tur risk att oönskad eller felaktig kod produktionssätts.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att säkerställa att beslutade rutiner för programförändringar följs oavsett utvecklingsform eller applikation. Riksrevisionen rekommenderar vidare Skatteverket att strukturera dokumentation av programförändringar så att en programförändring tydligt kan följas från beställning till produktionssättning.

2.2 Utvecklare har åtkomst till produktionsdatabaser

Riksrevisionen har under årets granskning, liksom tidigare år, noterat att för de fyra handläggningssystemen TINA, Moms AG, Skattekontot och Kuling har flera utvecklare även skrivrättigheter till produktionsmiljön och kan därmed göra ändringar i systemens produktionsdatabaser. Som nämns ovan finns det ingen systematisk uppföljning av om detta sker.
Att inte separera åtkomst mellan utvecklings- och produktionsmiljöer i programändringsflödet medför att en enskild individ på egen hand kan driftsätta en programförändring utan att beslutade kontroller har genomförts. Detta ökar risken för produktionssättning av såväl avsiktliga som oavsiktliga fel i system.

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 Skatteverket överväga att införa en generell rutin för uppföljning av utvecklares åtkomst till produktionsmiljöer för alla relevanta system.

DNR: 3.1.2-2017-0640
BESLUT: 2018-02-26

3. Övriga observationer

3.1 Säkerhetskopior förvaras inte geografiskt skiljt från driftstället

Riksrevisionen har noterat att säkerhetskopior från de applikationer som är produktionssatta i de två datahallarna SK1 och SK2 inte förvaras geografiskt åtskilt från produktionsdatat. Förvaring av säkerhetskopior på samma geografiska plats innebär en risk att både originaldata och säkerhetskopior kan förloras i samma incident.

Rekommendation
Riksrevisionen rekommenderar Skatteverket att säkerställa att säkerhetskopior av verksamhetskritisk data förvaras geografiskt åtskild från produktionsdata.

Ansvarig revisor Charlotte Ehrengren har beslutat i detta ärende. Granskningsledare Marcus Visser har varit föredragande.

Charlotte Ehrengren Marcus Visser

Kopia för kännedom:

Regeringen
Finansdepartementet
Finansdepartementet, budgetavdelningen