RIKSREVISIONEN

SKATTEVERKET
171 94 SOLNA

DNR: 3.1.2-2018-0570
BESLUT: 2019-04-12

Revisionsrapport – Granskning av generella IT-kontroller för ett urval av system vid Skatteverket 2018

Som en del av arbetet med att granska Skatteverkets årsredovisning 2018 har vi granskat vissa delar av den interna styrningen och kontrollen som bedömts vara relevant för vår revision.

Vi vill med denna revisionsrapport uppmärksamma er på iakttagelser från vår granskning av generella IT-kontroller för systemen Skattekontot, TINA, Moms AG och Kuling samt beräkningsmodulerna BD1000 och BD2000.

Vi vill att ni svarar på denna revisionsrapport senast 2019-05-17. Beskriv om och i så fall vilka åtgärder ni planerar för att rätta till de iakttagna bristerna.

Sammanfattning

Skatteverket har en mycket omfattande och komplex IT-miljö med IT-system som är väsentliga för verksamhetens drift såväl som för finansiell redovisning och resultatredovisning. 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 och kontroller för behörighetshantering, programförändringar och drift i myndighetens verksamhetskritiska IT-system.

Våra iakttagelser är:

1. *Brister i hanteringen av behörigheter*
   Det finns behov av att minska antalet användare med höga behörigheter i verksamhetskritiska system samt behov att förbättra rutinen för övervakning av dessa behörigheter.

2. *Brister i rutiner för programförändringar*
   Skatteverket bör verka för att separera användares åtkomst till utvecklings- och

produktionsmiljö. Skatteverket behöver också säkerställa att testning och godkännande utförs av olika personer även i beräkningsmodulerna BD1000 och BD2000.

3. *Brister i kontroller för drift av IT-system*
   - Säkerhetskopior förvaras inte geografiskt skiljt från driftstället
   - Avbrottsplan avseende IT-drift har inte testats under 2018
   - Systematiska återläsningstester av säkerhetskopierade data genomförs inte
   - Det finns ingen formell rutin för systemuppdatering av Linux-plattformen

Iakttagelserna avser endast rutiner och kontroller för de system som vi har granskat, men eftersom granskningen gäller generella IT-kontroller kan iakttagelserna och rekommendationerna vara aktuella även för andra system inom Skatteverket.

Riksrevisionen har även tidigare år granskade generella IT-kontroller hos Skatteverket. En del av våra iakttagelser återkommer.

1 Brister i hanteringen av behörigheter

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

Vår granskning har i år, likt tidigare år, visat att ett stort antal personer tillhör en hög behörighetsklass. För att få de rättigheter som denna behörighetsklass har, krävs dock även att användaren har ett så kallat smartkort för att få åtkomst till aktuell server. De rättigheter som denna behörighetsklass har, ger användaren möjlighet att påverka de granskade systemen. Påverkan på systemen kan för dessa behörigheter dessutom vara svåra att spåra.

Många användare med denna höga behörighetsklass kan innebära ökad risk för obehörig åtkomst till program och information. Det kan också öka risken för felaktigheter och misstag på grund av okunskap, slarv eller oegentligheter.

Riksrevisionen är medveten om att Skatteverket fortsatt bedriver ett arbete för att åtgärda detta, men vid årets granskning kvarstår dock iakttagelsen. Enligt uppgift från Skatteverket kan det med nuvarande systemdesign vara svårt att minska antalet personer som tillhör denna höga behörighetsklass.

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

I SKV:s miljö innebär domänadministratörsrollen bland annat risk att de tilldelar icke godkända behörigheter till personer (inklusive sig själv) som inte ska ha sådan behörighet i verksamhetens system.

Av Skatteverkets svar på motsvarande iakttagelse i föregående års rapport, framgår att myndigheten avser införa tidsbegränsade behörigheter för domänadministratörer. Vi har i granskningen inte kunnat konstatera att tidsbegränsade behörigheter är införda.

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. Det 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 i Active Directory. Dessa loggar lagras under en längre tidsperiod, på ett vad vi förstår systematiskt och strukturerat sätt. Skatteverket utför 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 i applikationer och databaser.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att definiera och införa en riskbaserad rutin för kontinuerlig uppföljning, av 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 Utvecklare har åtkomst till produktionsdatabaser

Vi 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. Det innebär att de kan göra ändringar i systemens produktionsdatabaser. Som nämns ovan finns det ingen systematisk uppföljning av loggar om detta sker.

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

Av Skatteverkets svar på motsvarande iakttagelse i föregående års rapport, framgår att myndigheten avser att ändra skrivrättigheter till läsrättigheter för dessa utvecklare. I de fall skrivrättigheter behövs kommer en rutin för att söka temporär skrivrättighet att införas. Vi har i årets granskning inte kunnat konstatera att dessa åtgärder har införts.

Rekommendation

Riksrevisionen rekommenderar därför fortsatt Skatteverket att genomföra de planerade åtgärderna.

2.2 Avsaknad av rollfördelning för BD1000 och BD2000

Vid årets granskning av rutiner för programförändringar för BD1000 och BD2000 har vi observerat att det är samma person som både testar och godkänner produktionssättning.

En avsaknad av ansvarsfördelning innebär att den som har testat programförändringar även utvärderar och kvalitetssäkrar sitt eget arbete. Att en person ensam gör test och sedan bedömer testresultatet ökar risken för att felaktiga förändringar driftsätts i produktionsmiljön. Det ökar också risken för nyckelpersonberoende, då få personer tar en aktiv del i processen.

Rekommendation

Riksrevisionen rekommenderar att Skatteverket säkerställer att testning och godkännande utförs av olika personer även för BD 1000/2000.

3 Brister i kontroller för drift av IT-system

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 förvara säkerhetskopior av verksamhetskritiska data geografiskt åtskild från produktionsdata.

3.2 Avbrottsplan avseende IT-drift har inte testats under 2018

Vid granskningen framkom att Skatteverket inte har genomfört ett test av sin avbrottsplan för IT-drift under 2018.

Att inte testa avbrottsplanen innebär en ökad risk att planen inte är anpassad till den verksamhet som den omfattar. Det ökar också risken att ansvariga saknar kunskap för att utföra sina planerade åtgärder. Det finns även en risk att tillgång till verksamhetskritiska system fördröjs i händelse av en allvarlig incident.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att definiera och införa rutiner för periodisk test av avbrottsplan, utifrån bedömd risk. Berörd personal bör även utbildas i sina uppgifter enligt de framtagna rutinerna.

3.3 Systematiska återläsningstester av säkerhetskopierade data genomförs inte

Riksrevisionen har noterat att återläsningstester av data från backuper inte gjorts systematiskt under året. Vi har dock observerat att vissa applikationer, med viss regelbundenhet återläser sina egna data i samband med system- och acceptanstester. Det saknas dock en formell rutin som säkerställer att alla verksamhetskritiska system omfattas samt hur ofta detta ska ske.

Om återläsning av backuper inte testas finns risk att säkerhetskopiorna inte kan återläsas fullständigt och riktigt vid behov.

Rekommendation

Riksrevisionen rekommenderar Skatteverket att definiera och införa rutin för systematiska och periodiska återläsningstester av säkerhetskopior av produktionsdata för kritiska system.

3.4 Det finns ingen formell rutin för systemuppdatering av Linux-plattformen

Riksrevisionen har noterat att det inte finns en formell rutin för att hantera så kallad patchning av Linux-plattformen för de granskade systemen. Det innebär att vi inte har kunnat verifiera om Skatteverket bedömt nödvändigheten av att införa relevanta program- och säkerhetspatchar.

Avsaknaden av formella rutiner kring patchning innebär en ökad risk att man brister i sin omvärldsbevakning och därför inte inför uppdateringar som är av väsentlig betydelse.

DNR: 3.1.2-2018-0570
BESLUT: 2019-04-12

Rekommendation

Riksrevisionen rekommenderar Skatteverket att införa en formell rutin för patchhantering och att systematiskt dokumentera den omvärldsbevakning som sker och vilka slutsatser som tagits kring släppta uppdateringar.

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