RIKSREVISIONEN

SKATTEVERKET
171 94 SOLNA

DNR: 3.1.2-2020-0461
BESLUT: 2021-03-18

Revisionsrapport – Brister i generella it-kontroller

Som en del av arbetet med att granska Skatteverkets årsredovisning 2020 har vi granskat vissa delar av den interna styrningen och kontrollen som bedömts vara relevant för revisionen.

Vi vill med denna revisionsrapport uppmärksamma er på iakttagelser från vår granskning av generella it-kontroller. Granskningen omfattar de it-system som är relevanta för vår granskning av viktiga verksamhetsprocesser, så som inkomstskatt, arbetsgivaravgifter, moms och punktskatt.

Vi vill att ni svarar på denna revisionsrapport senast 2021-04-16. Beskriv om och i så fall vilka åtgärder ni planerar för att rätta till iakttagelserna.

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 över verksamhetskritiska it-system.

Vi bedömer att det finns behov av att stärka den interna kontrollen inom några områden, vilket vi också rapporterat vid tidigare granskningar. Vi konstaterar att Skatteverket under året har infört åtgärder och påbörjat aktiviteter som syftar till att stärka den interna kontrollen, men att iakttagelserna ännu inte åtgärdats fullt ut.

Vi har noterat följande:

1. Kontroller över höga it-behörigheter bör stärkas.
2. Utvecklare har åtkomst till produktionsdatabaser.
3. Behörighetsadministration - periodisk kontroll omfattar inte alla behörigheter och administratörer kan tilldela behörigheter till sig själva.
4. Rutiner för att återskapa information i händelse av en katastrof bör stärkas.

5. Bristande spårbarhet vid programförändringar i systemen för moms och arbetsgivaravgifter.

Övriga iakttagelser i samband med granskningen av generella it-kontroller är av mindre allvarlig karaktär varför vi har lämnat dessa muntligen till Skatteverket.

1. Kontroller över höga it-behörigheter bör stärkas

Vår granskning har i år, likt tidigare år, visat att ett stort antal personer tillhör en hög behörighetsklass. De rättigheter som denna behörighetsklass har, ger användaren möjlighet att göra omfattande ändringar i de granskade systemen. Ändringar i systemen som görs med dessa behörigheter kan dessutom vara svåra att spåra.

Många användare med denna höga behörighetsklass kan innebära ökad risk för obehörig åtkomst till program och information. Det kan öka risken för avsiktliga eller oavsiktliga fel.

Vi är medvetna om att Skatteverket fortsatt bedriver ett arbete för att åtgärda risken och vi noterar en minskning av antalet användare med denna behörighet sedan förra årets granskning. Vi noterar också att riskreducerande åtgärder såsom loggning, uppföljning och övervakning har stärkts. Vår bedömning vid granskningstillfället är dock att samtliga åtgärder fortfarande inte är fullt införda.

Rekommendationer

Vi rekommenderar Skatteverket att fortsätta

- arbetet med att begränsa antalet användare med denna höga behörighetsklass
- arbetet med att införa riskreducerande åtgärder.

2. Utvecklare har åtkomst till produktionsdatabaser

Vi har under årets granskning, likt tidigare år, noterat att flera utvecklare även har skrivrättigheter i produktionsmiljön. Det innebär att de kan göra ändringar i systemens produktionsdatabaser. Det finns 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 systemen.

Rekommendation

Vi rekommenderar Skatteverket att genomföra åtgärder för att hantera risken för felaktiga ändringar i produktionsmiljön.

3. Behörighetsadministration - Periodisk kontroll omfattar inte alla behörigheter och administratörer kan tilldela behörigheter till sig själva

Vi har vid granskningen noterat ett behov av att stärka kontrollerna över behörighetsadministrationen. Vi har noterat att alla användarkonton inte ingår i den årliga periodiska kontrollen av behörigheter (återgodkännande). Det gäller till exempel användarkonton för

- behörighetsadministratörer
- anställda på Statens Service Center med behörigheter i Skatteverkets it-system.

Vi har även noterat att behörighetsadministratörer har teknisk möjlighet att tilldela behörigheter till sig själva.

Detta innebär en risk att användare har behörigheter som de inte behöver för att utföra sitt arbete, vilket ökar risken för avsiktliga eller oavsiktliga fel.

Rekommendationer

Vi rekommenderar Skatteverket att

- införa periodisk kontroll som omfattar alla behörigheter
- införa kompletterande kontrollåtgärder över de behörighetskonton som har möjlighet att tilldela behörigheter till sig själva.

4. Rutiner för att återskapa information i händelse av en katastrof bör stärkas

Vi har vid tidigare års granskning noterat behov av att stärka rutinerna för återskapande av information i händelse av driftsavbrott eller katastrof. Det gäller uppdatering och testning av avbrottsplaner samt förvaring och testning av säkerhetskopior.

Svagheter inom dessa områden medför en ökad risk att tillgång till verksamhetskritiska system fördröjs samt att information förloras i händelse av ett driftsavbrott eller katastrof.

Vi har vid årets granskning blivit informerad om att Skatteverket har påbörjat aktiviteter för att hantera riskerna men att dessa inte är fullt ut införda.

Rekommendation

Vi rekommenderar Skatteverket att fortsätta arbetet med att stärka kontrollerna för att hantera risker vid driftsavbrott eller katastrof.

5. Bristande spårbarhet vid programförändringar i systemen för moms och arbetsgivaravgifter

Vi har noterat brister i spårbarhet och dokumentation av programförändringar av systemen för moms och arbetsgivaravgifter. För flertalet ändringar saknar Skatteverket till exempel

- dokumentation av de tester som utförts
- godkännande, inför att förändringarna driftsatts.

Brister i spårbarhet gör det svårt att verifiera att aktiviteter och kontroller har genomförts med förväntad kvalitet för att säkerställa att felaktig kod inte installerats i produktion. Det skapar också ett personberoende som riskerar att försvåra vid felsökning och kunskapsöverföring.

DNR: 3.1.2-2020-0461
BESLUT: 2021-03-18

Rekommendation

Vi rekommenderar att Skatteverket tydliggör dokumentationskrav för att säkerställa spårbarhet genom hela programförändringsprocessen.

Ansvarig revisor Charlotte Ehrengren har beslutat i detta ärende. IT-revisor Helen Lagerholm har varit föredragande.

Charlotte Ehrengren

Helen Lagerholm

Kopia för kännedom:

Regeringen
Finansdepartementet