RIKSREVISIONEN

STATENS TJÄNSTEPENSIONSVERK
851 90 SUNDSVALL

DNR: 3.1.2-2017-0667
BESLUT: 2018-04-20

Statens tjänstepensionsverk

Revisionsrapport – Granskning av rutiner och kontroller för behörigheter och systemförändringar inom IT 2017

Som ett led i granskningen av årsredovisningen med syfte att göra uttalanden om denna, har Riksrevisionen även granskat vissa delar av den interna styrningen och kontrollen som bedömts vara relevant för revisionen. Denna granskning syftar till att verifiera hur Statens tjänstepensionsverk (SPV) 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.

De punkter som framgår i revisionsrapporten är sådana iakttagelser som vi har identifierat och som Riksrevisionen vill fästa ledningens uppmärksamhet på.

Riksrevisionen önskar information senast 2018-06-20 med anledning av våra iakttagelser i denna rapport.

Iakttagelse 1: Stort antal individer innehar höga behörigheter

Vid vår granskning noterar vi att i både stordatormiljön och windowsmiljön finns relativt många individer med höga IT-behörigheter. Vår bedömning är att ett för stort antal användare med hög IT-behörighet inte är förenligt med god intern kontroll avseende IT.

Användare med hög åtkomst kan påverka funktioner och/eller data vilket kan öka risken för felaktigheter och misstag på grund av okunskap, slarv eller oegentligheter. Hög åtkomst i systemen bör vara begränsad till användare som behöver detta för sina arbetsuppgifter.

Riksrevisionen *rekommenderar* SPV att analysera behovet av användare med hög behörighet i systemen och begränsa antalet till användare som behöver detta för sina arbetsuppgifter. Detta gäller både egen personal, anlitade konsulter och driftleverantörernas personal.

Iakttagelse 2: Brister i design av regelbunden uppföljning av behörighet

SPV har tagit steg framåt i den kontroll som innebär att genomföra periodiska uppföljningar av alla höga behörigheter. Dock noterar vi i årets granskning att det finns vissa otydligheter gällande hur denna kontroll ska utföras. Det saknas en tydlig rutinbeskrivning där det framgår vilka behörigheter som ska följas upp, hur ofta de ska kontrolleras och vem som ska genomföra kontrollen. När detta är otydligt ökar risken för att kontrollen inte genomförs på rätt sätt eller inte genomförs alls. Att inte genomföra periodisk uppföljning av behörigheter ökar risken för att fel i behörighetshanteringen inte fångas upp. Detta kan i sin tur innebära ökad risk för obehörig åtkomst till program och information. Det ökar även risken för att personer som bytt roll inom SPV innehar känsliga behörighetskombinationer som inte upptäcks.

Riksrevisionen *rekommenderar* SPV att analysera hur kontrollen ”periodiska behörighetsgenomgångar” ska utformas för att säkerställa lämplig behörighetshantering med fokus på höga behörigheter inom IT.

Ansvarig revisor Agneta Bergman har beslutat i detta ärende. Uppdragsledare Anette Sannebro har varit föredragande.

Agneta Bergman

Anette Sannebro