DNR: 32-2014-0428

FÖRSÄKRINGSKASSAN
103 51 STOCKHOLM

BESLUT: 2015-04-10

Granskning av rutiner och kontroller för behörigheter och systemförändringar inom IT

Riksrevisionen har som ett led i den årliga revisionen av Försäkringskassan granskat rutiner och kontroller inom IT som syftar till att säkerställa 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. Granskningen har omfattat en stor del av de system som används för handläggning av socialförsäkringar vid Försäkringskassan.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa Försäkringskassans lednings uppmärksamhet på med denna revisionsrapport.

Riksrevisionen önskar information senast 2015-05-08 med anledning av våra iakttagelser i denna rapport.

Transcendent group AB (TGAB) har biträtt Riksrevisionen i denna granskning. TGAB har avrapporterat sin genomförda granskning till Riksrevisionen. Av bilaga 1 framgår samtliga iakttagelser som gjorts vid denna granskning. Iakttagelserna har sorterats in under de iakttagelser som rapporterades till Försäkringskassan vid förra årets revision och utgör därmed även en uppföljande beskrivning av hur dessa iakttagelser utvecklats sedan dess.

De främsta iakttagelserna och rekommendationerna är:

- Försäkringskassan tillämpar inte samma rutiner för förändringar i COBOL-baserad programvara som för övrig programvara. Existerande rutiner för ändringar i COBOL-baserade system bör tydligare säkerställa en separation mellan utvecklare och testare. En positiv utveckling av kontrollerna har genomförts under 2014 genom att införa krav på dokumenterade testprotokoll även för dessa systemförändringar. Riksrevisionen rekommenderar att rutinen bättre säkerställer dualitet. Se punkt 5.3 i bilaga 1.
- Försäkringskassan rekommenderas att införa programmerade kontroller som säkerställer att endast behörig chef kan beställa behörigheter. Vidare bör fråga om känsliga kombinationer av behörigheter inom förmånssystemen utredas och programmerade kontroller införas i syfte att undvika att sådana läggs in i systemen. Förberedande aktiviteter för att åtgärda dessa iakttagelser pågår vid Försäkringskassan. Riksrevisionen

rekommenderar Försäkringskassan fortsatt att bevaka utvecklingen av dessa aktiviteter. Se punkt 5.6 i bilaga 1.

- Granskningen visar att styrning och uppföljning av behörigheter för IT-personal under 2014 inte varit formaliserad i den utsträckning som torde vara nödvändig för att säkerställa god intern kontroll. Vi noterar att ett utvecklingsarbete vid Försäkringskassan har pågått under 2014, med ett införande under slutet av året. Riksrevisionen rekommenderar att detta införande fullföljs. Se punkt 5.10 samt 5.13 i bilaga 1.

Ovan punkter beskrivs mer utförligt i bilaga 1 som även innehåller ett antal andra iakttagelser av något mindre dignitet. Försäkringskassan rekommenderas att ta del även av dessa och överväga vilka åtgärder som behövs.

Ansvarig revisor Stefan Gollbo har beslutat i detta ärende. Granskningsledare Erik Jäder har varit föredragande

Stefan Gollbo Erik Jäder