DNR: 32-2013-0435

FÖRSÄKRINGSKASSAN
103 51 STOCKHOLM

BESLUT: 2014-04-11

# 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 uppmärksamhet på med denna revisionsrapport.

Riksrevisionen önskar information senast 2014-05-19 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. TGAB:s rapport visar att de kontroller som granskats överlag bedöms vara effektiva, men granskningen visar också att det finns ett antal brister där åtgärder behöver vidtas. TGAB:s rapport biläggs i dess helhet till denna rapport. 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 ses över och bland annat rekommenderas en tydligare separation mellan utvecklare och testare. Se avsnitt 5.3 i den bilagda rapporten.
- Brister avseende dokumentation av tester inför införande av systemförändringar har noterats. En genomgång och uppföljning av rutiner för tester samt dokumentation av utförandet rekommenderas, se avsnitt 5.5 i den bilagda rapporten.
- 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. Se avsnitt 5.6 i den bilagda rapporten.
- Granskningen visar att styrning och uppföljning av behörigheter för IT-personal inte är formaliserad i den utsträckning som torde vara nödvändig för att säkerställa god intern

DNR: 32-2013-0435

FÖRSÄKRINGSKASSAN
103 51 STOCKHOLM

BESLUT: 2014-04-11

kontroll. Rutinen behöver formaliseras i större utsträckning och vi noterar att ett utvecklingsarbete vid Försäkringskassan pågår. Riksrevisionen rekommenderar att detta fullföljs och införs. Se avsnitt 5.9, 5.10 samt 5.13 i den bilagda rapporten.

Ovan punkter beskrivs mer utförligt i den bilagda rapporten som även innehåller ett antal andra iakttagelser av mindre karaktär. Försäkringskassan rekommenderas att ta del även av dessa och överväga vilka åtgärder som behövs.

Ansvarig revisor Stefan Gollbo har beslutat i detta ärende. Uppdragsledare Agneta Bergman har varit föredragande

Stefan Gollbo Agneta Bergman

Kopia för kännedom:

*Regeringen*
*Socialdepartementet*
*Finansdepartementet, budgetavdelningen*