



## Försäkringskassan

# Revisionsrapport – Granskning av rutiner och kontroller för behörigheter och systemförändringar inom IT 2015

Som ett led i granskningen av årsredovisningen med syfte att göra uttalanden om denna har Riksrevisionen även granskat rutiner och kontroller inom IT. Denna granskning syftar till att verifiera hur Försäkringskassan 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. Granskningen har omfattat en stor del av de system som används för handläggning av socialförsäkringar vid Försäkringskassan. Granskningen har även omfattat de av Pensionsmyndighetens system som driftsmässigt hanteras av Försäkringskassan, därför skickas en kopia av denna revisionsrapport för kännedom till Pensionsmyndighetens ledning.

Nedan punkter är iakttagelser som Riksrevisionen vill fästa ledningens uppmärksamhet på. En redogörelse för samtliga iakttagelser har lämnats till berörda inom Försäkringskassan.

Riksrevisionen önskar information senast 2016-07-04 med anledning av våra iakttagelser i denna rapport.

### *Iakttagelse 1: Informella rutiner och otydlighet kring högre (priviligierade) IT-behörigheter*

Försäkringskassans processer för hantering av IT-behörigheter inom enskilda teknikområden är fortsatt informella. Det innebär en sämre förmåga av spårbarhet för tilldelade behörigheter samt en högre risk för onödig förekomst av känsliga behörigheter. Risk finns också att behörigheter beställs av personer som inte bör kunna beställa vissa typer av behörigheter. Vi noterar att ett utvecklingsarbete för att höja kontrollnivån har pågått under 2014 och 2015, detta är under införande vid Försäkringskassan.

*Riksrevisionen rekommenderar att detta införande fullföljs.*

*lakttagelse 2: Brister i regelbunden uppföljning av särskild och privilegierad behörighet*

Försäkringskassan genomför inte generellt periodiska genomgångar av särskilda och privilegierade behörigheter. Att periodiska genomgångar inte görs ökar risken för att behörigheter som bör tas bort finns kvar. Detta ökar i sin tur bland annat risken för att personer som bytt roll inom Försäkringskassan innehar känsliga behörighetskombinationer som inte upptäcks.

*Riksrevisionen rekommenderar* fortsatt Försäkringskassan att säkerställa periodiska behörighetsgenomgångar för särskilda och privilegierade behörigheter inom IT.

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

Agneta Bergman

Anette Sannebro

Kopia för kännedom:

*Pensionsmyndigheten*