



Arbetsförmedlingen

Revisionsrapport – Granskning av generella IT-kontroller

Riksrevisionen har som ett led i den årliga revisionen av Arbetsförmedlingen granskat IT-kontroller i ett urval av myndighetens väsentliga transfereringsflöden. Granskningen har omfattat de system som används för redovisning och utbetalning av olika former av ersättningar samt bidrag.

Riksrevisionens granskning har genomförts i två delar där den första delen fokuserat på processspecifika kontroller vilka syftar till att säkerställa en fullständig och riktig redovisning. Denna del av granskningen har utförts utan anmärkningar. Riksrevisionen har även utfört en standardmässig kartläggning och testning av generella IT-kontroller i två IT-system vilka är väsentliga för redovisning och utbetalning av ersättningar samt bidrag. De IT-system som har granskats är redovisningssystemet Raindance och bidragshanteringssystemet Åtgärd. Granskningen har omfattat rutiner och kontroller för systemförändringar, behörighetshantering och IT-drift.

De punkter som framgår i revisionsrapporten är sådana iakttagelser som Riksrevisionen vill fästa ledningens uppmärksamhet på. Iakttagelserna avser endast rutiner i de två system som har granskats, eftersom granskningen gäller generella IT-kontroller kan de vara aktuella att beakta även för andra system inom myndigheten.

Riksrevisionen önskar information senast 2016-06-24 med anledning av våra iakttagelser i denna rapport.

Gruppkonto används för åtkomst till databaser i Raindance och Åtgärd

Vid inloggning till databaserna i systemen Raindance och Åtgärd använder databasadministratörer ett gruppkonto. Med gruppkonto menas att flera personer använder ett och samma användarkonto. Anställda och konsulter med kunskap om gruppkontots lösenord får åtkomst till databaserna. Användning av gruppkonton försvårar möjligheten till god intern styrning och kontroll. Det är exempelvis svårt att i efterhand spåra vem som utfört ändringar i systemen.

Rekommendation

Riksrevisionen rekommenderar Arbetsförmedlingen att genomgående använda unika användarkonton som är kopplade till enskilda personer och som möjliggör spårbarhet.

Användare har möjlighet att både utveckla och produktionssätta programkod i Åtgärd

Granskningen har visat att fem användare har behörighet att produktionssätta programkod avseende Åtgärd samtidigt som de har tillgång till arkiv för programkod. Detta möjliggör för användaren att såväl utveckla som produktionssätta programkod för Åtgärd.

Bristande arbetsfördelning av uppgifter i programändringsflödet medför att en enskild individ på egen hand kan genomföra en programförändring. Detta ökar risken för såväl avsiktliga som oavsiktliga fel.

Rekommendation

Riksrevisionen rekommenderar Arbetsförmedlingen att tillse att användare som har höga behörigheter och som kan driftsätta programkod inte samtidigt har tillgång till arkiv för programkod.

Ansvarig revisor Björn Sande har beslutat i detta ärende. Uppdragsledare Iréne Lindström har varit föredragande.

Björn Sande

Iréne Lindström

Kopia för kännedom:

Regeringen

Arbetsmarknadsdepartementet

Finansdepartementet, budgetavdelningen