Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.2	Systemgenererade listor över applikations-förändringar kan för närvarande inte produceras.	Avsaknad av fullständiga listor över applikationsförändringar som har driftsatts innebär att det finns begränsade möjligheter att kontrollera att alla applikationsförändringar som driftsätts följer myndighetens processer och kontroller för applikationsförändringar, d.v.s. det skydd som myndigheten har implementerat. Detta ökar risken för att oönskade förändringar driftsätts utan att upptäckas, vilket kan leda till ökade kostnader på grund av avbrott i kritiska system. Vidare försvårar brister i spårbarheten uppföljning i samband med t.ex. felsökning.	Låg	I samband med migrering av ett leveransverktyg så avser vi att införa funktionalitet som automatiskt genererar listor på driftsatta applikationsförändringar. Detta kommer ske under 2014.
5.2 Status vid revisionens genomförande 1-2 dec 2014: Lösningen är inte helt implementerad och beräknas kunna börja användas fullt ut från årsskiftet 2014/2015.				

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.3	Osäker ändringsrutin för standardändringar i COBOL.	Avsaknaden av godkännanden för utveckling och produktionssättning samt det faktum att ändringar kan utvecklas och testas av samma person ökar risken för att otillräckligt testade eller icke avsedda ändringar förs in i produktmiljön.	Medel	För att säkerställa att samtliga applikationsändringar är testade inför produktionssättning kommer en processförändring genomföras där en kontroll i QA-funktionen inom ITPL införs, vilket innebär att till samtliga ändringsbegäran (RFC) ska en testrapport vara bifogad. Saknas testrapport så avslås ändringsbegäran. Processförändringen kommer att införas under juni 2014 och kommer att avrapporteras till kvalitetsansvarig ITP månadsvis. Enligt ”Riktlinje för test, revision E” (beslutad 2009-10-01) framgår vilken roll som utför vilket arbete. Med en uppdelning mellan utvecklingsrollerna ADI och Test har Försäkringskassan ett arbetssätt som undviker att samma resurs både utvecklar och testar levererad funktionalitet. Utifrån den identifierade risken har ett förtydligande gått ut till samtliga utvecklingsteam inom IT-avdelningen, där vikten av att inte samma resurs både utvecklar och testar levererad funktionalitet har poängterats. För att kontrollera att detta efterlevs kommer stickprovskontroller att göras vid ett par tillfällen per år. Tillämpningen av processerna för utveckling och test kommer också att förtydligas. Uppföljning av projekt- och bemanningsplaner samt ändrings- och testprotokoll ska ske kvartalsvis med start under 2014-Q3.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014

5.3 Status vid revisionens genomförande 1-2 dec 2014:
Iakttagelsen från föregående år kvarstår delvis, det noteras även att det *behörighetsmässigt* är möjligt att en applikationsförändring utvecklas och testas av samma person. Enligt gällande *rutiner* ska dock en applikationsförändring utvecklas och testas av olika personer.

Vi rekommenderar Försäkringskassan fortsatt att se över ändringsrutinerna för COBOL-ändringar. Då Försäkringskassan sedan 1 juli 2014 kräver testprotokoll för alla typer av förändringar bör Försäkringskassan utvärdera möjligheten att samordna kontrollen av testprotokoll med ett formellt godkännande för produktionssättning för att säkerställa att icke avsedda eller otillräckligt testade COBOL-ändringar ej produktionssätts samt att utveckling och test har utförts av olika personer.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.4	Bristande tydlighet i hur nödvändiga testnivåer fastställs.	Att Försäkringskassan inte har ett dokumenterat stöd för fastställande av nödvändiga testnivåer ökar risken för att otillräckligt testade applikationsförändringar införs i myndighetens produktionsmiljö. Det kan leda till att funktionalitet i kritiska system påverkas på ett oönskat sätt vilket vidare kan orsaka att dessa system räknar fel utan att det upptäcks.	Låg	Försäkringskassan har i ”Riktlinje för test, revision E” (beslutad 2009-10-01) beskrivit de testnivåer som finns och används (se sid 14-25) och mer utförligt i ”Testnivåer och typer av fel”. Vad som ska testas på vilken nivå beror bl.a. på vilken teknisk plattform som utveckling bedrivs på, utvecklingsstrategi, om man har riskbaserad strategi, typ av förändring osv. Utöver testriktlinjerna så är alla anställda testare certifierade enligt ISTQB:s internationella standard för mjukvarutestning samt har genomgått den interna testutbildningen. Den interna utbildningen går bl.a. nogsamt igenom hur man fastställer vad som ska testas på vilken testnivå utifrån ovanstående nämnda parametrar. Dessutom gås alla testrollers ansvar och uppdrag igenom. Hur man fastställer de olika testnivåerna kommer inte att finnas att tillgå i testriktlinjerna eftersom det inte går att i allmänna termer göra en relevant beskrivning. Dokumentation för testnivåer (Testriktlinjer samt Testnivåer och typer av fel) samt rollbeskrivningar finns publicerade på Försäkringskassans intranät. Det är testledaren som ansvarar för planeringen, vilket finns beskrivet i rollbeskrivningen. Under hösten 2014 kommer en översyn att göras för att säkra att all dokumentation finns samlad på ett ställe samt att senaste versionen finns publicerad.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.4 Status vid revisionens genomförande 1-2 dec 2014: Under 2014 har Försäkringskassan uppdaterat sina testriktlinjer[1] för att få dem mer lättarbetade. Däremot finns fortfarande ingen dokumentation som specificerar nödvändiga testnivåer för olika typer av aktiviteter och system, alternativt en rutinbeskrivning för hur nödvändiga testnivåer ska fastställas. Vi rekommenderar fortatt att Försäkringskassan dokumenterar nödvändiga testnivåer för olika typer av ändringar för olika system, alternativt annat stöd för beslut om nödvändiga testnivåer.				

[1] Testriktlinjer Försäkringskassan ITA (2014-10-13)

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.5	Bristande spårbarhet gällande testning av applikationsförändringar.	Bristande spårbarhet i applikationsförändringsprocessen gällande testning försvårar arbetet vid en eventuell felsökning. Risken ökar även för att fel oavsiktligt förs in i produktionsmiljön på grund av oaktsamhet.	Hög (2013) Medel (2014)	Rent generellt har Försäkringskassan en fungerande process/arbetssätt för testningen av applikationsförändringar. Vid revisionstillfället har det framkommit ett antal standardförändringar i Cobol där utvecklingsteamen inte kunnat uppvisa testdokumentation. Enligt vår testmetodik ska förändringar testas och dokumenteras i en testrapport. Utifrån identifierad brist har ett förtydligande gått ut till samtliga utvecklingsteam att testrapport ska finnas för samtliga applikationsförändringar. För att säkerställa att samtliga applikationsändringar är testade inför produktionssättning kommer en processförändring att genomföras där en kontroll i QA-funktionen inom ITPL införs, vilket innebär att till samtliga ändringsbegäran (RFC) ska en testrapport vara bifogad. Saknas testrapport så avslås ändringsbegäran. Processförändringen kommer att införas under juni 2014 och kommer att avrapporteras till kvalitetsansvarig ITP månadsvis.

5.5 Status vid revisionens genomförande 1-2 dec 2014:

För 11 av 30 testade förändringar har vi inte kunnat ta del av någon dokumentation som visar på att testning är genomförd. Samtliga av dessa är COBOL-förändringar utförda fram till och med juni 2014 innan rutin infördes att test-protokoll ska sparas och bifogas i ARS. För de förändringar som införts i produktionsmiljön efter 1 juli 2014 fanns testprotokoll för de granskade förändringarna.

Vi rekommenderar att Försäkringskassan fortsätter att genomföra kontroller enligt den nya rutin som infördes 1 juli 2014 för att säkerställa att testdokumentation upprättas och sparas.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.6	Otillräckliga automatiska kontroller vid behörighetsbeställning i BOA.	Att behörigheter kan beställas av personer som inte är berättigade att beställa till en given medarbetare ökar risken för att behörigheter felaktigt tilldelas personer som inte är i behov av dessa i sitt arbete. Risken ökar också för att det förekommer känsliga behörighetskombinationer som till exempel kan sätta viktiga dualitetkontroller ur spel.	Medel	Ett VBB (verksamhetens behovsbeskrivning) är framtaget och ett projekt gällande översyn av organisationsstrukturen i behörighetssystemet för delar av FK är under planering. Tillrättaläggandet av dessa delar löser delvis problematiken med att BOA (Administration av Behörighet, Organisation och Användare) inte automatiskt kontrollerar att beställare är närmast verksamhetsansvarig chef. Ett VBB kommer att skrivas under Q2 2014 som adresserar möjligheten att utöka funktionaliteten i BOA för att möta Riksrevisionens rekommendation 5.6.3.

5.6 Status vid revisionens genomförande 1-2 dec 2014:
Enligt Försäkringskassan har ett VBB (verksamhetens behovsbeskrivning) tagits fram för att åtgärda dessa punkter. Vid granskningstillfället fanns det dock ej något beslut i frågan. Vidare pågår en förstudie för systemstöd för behörighetsadministrationen med krav på automatiska kontroller av otillåtna kombinationer.

Vi rekommenderar att Försäkringskassan utreder möjligheterna att utöka BOA:s funktionalitet att inkludera spärrar som gör att endast berättigad chef kan beställa behörigheter samt en kontroll som varnar vid beställning av behörigheter som skapar otillåtna eller känsliga kombinationer.

Vidare rekommenderar vi Försäkringskassan att utreda vilka kombinerade behörighetskombinationer i förmånssystemens befintliga roller och profiler som ej är tillåtna enligt givna beslut och riktlinjer för informationssäkerhet.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.7	Avsaknad av systemstöd för tidsbestämda borttag av behörigheter och konton.	Att systemstöd saknas för att automatiserat stänga av konton eller ta bort behörigheter från ett tidsbestämt datum, vilket ökar risken för att personer som bytt roll eller avslutat sin anställning inom Försäkringskassan fortsatt innehar känsliga behörighetskombinationer.	Låg	Rekommendationen 5.7.3. kommer att adresseras genom projektet ”Personaldata” som levererar en systemlösning 1 juni 2014 för automatisk låsning/borttag av konton utifrån anställningens/uppdragets ”t.o.m. datum”. Systemstöd för att kunna tidsstyra behörigheter som idag ligger utanför BOA kommer att utredas i en förstudie som är planerad under andra halvåret 2014.

5.7 Status vid revisionens genomförande 1-2 dec 2014:

Under september 2014 har funktion implementerats för automatisk låsning av användarkonton för system inom BOA utifrån datum för tidsbunden anställning eller projekt. Dock saknas fortfarande systemstöd för tidsbestämt borttag av behörigheter utanför BOA.

Enligt Försäkringskassan pågår en förstudie fram till och med Q2 2015 avseende systemstöd för behörighetsadministration där krav på funktionalitet av tidsbestämd behörighet finns med.

Vi rekommenderar Försäkringskassan att utreda möjligheterna att införa systemstöd för att vid beställning av borttag av behörigheter i system utanför BOA kunna tidsbegränsa och styra borttag av behörigheter eller låsning av konto.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.8	Ingen spårbarhet i förändringar av Attest- och delegationsordningen.	Då Attest- och delegationsordningen sparas som en Excelfil utan spårbarhet bakåt finns risk för att den ändras felaktigt utan att man kan säkerställa vilka förändringar som gjorts, vilket ökar risken för att man inte kan identifiera obehöriga beställningar av behörighetsförändringar bakåt i tiden.	Låg	Otillräckligt systemstöd finns i dagsläget för att lösa problematiken. Försök att skapa acceptabel spårbarhet med nuvarande applikation har inte lyckats. Ett VBB (verksamhetens behovsbeskrivning) gällande systemstöd som adresserar rekommendationen 5.8.3 kommer att skrivas under Q2 2014.

5.8 Status vid revisionens genomförande 1-2 dec 2014:

Enligt Försäkringskassan har ett VBB (verksamhetens behovsbeskrivning) tagits fram för att åtgärda dessa punkter. Vid granskningstillfället fanns det dock ej något beslut i frågan.

Vi rekommenderar Försäkringskassan att införa ett system som tillåter versionshantering av Attest- och delegationsordningen för att säkerställa tillräcklig spårbarhet vid förändringar bakåt i tiden.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.9	Avsaknad av säkerhetsprövning för personal med höga IT-behörigheter.	Avsaknad av säkerhetsprövning av särskilda roller kan innebära risk för att man inte identifierar personal som ej är pålitlig ur säkerhetssynpunkt, är särskilt sårbar på grund av dubbla lojaliteter eller om det finns risk för att personen hamnar i en intressekonflikt eller utsätts för påtryckningar.	Medel (2013) Låg (2014)	Försäkringskassan har fattat beslut om att nämnda roller är placerade i säkerhetsklass. Säkerhetsprövning av medarbetare som är aktuella för rollerna pågår och beräknas vara klar den 1 september 2014. Samtliga konsulter med uppdrag som är placerade i säkerhetsklass har genomgått säkerhetsprövning. Cheferna ska varje år i samband med medarbetarsamtal med medarbetare som är placerade i säkerhetsklass även gå igenom frågorna i det personliga samtalet som ingår i säkerhetsprövningen.

5.9 Status vid revisionens genomförande 1-2 dec 2014:

Detta har genomförts enligt intervjusvar.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.10	Informella rutiner och otydlighet kring priviligierade IT-behörigheter.	De informella processer för behörighetshantering som används av de enskilda teknikområdena samt det faktum att oklarheter finns kring vilka behörigheter som ska tilldelas av IT innebär minskad kontroll gällande spårbarheten för tilldelade behörigheter och en ökad risk för att personer har känsliga behörigheter utan föreliggande behov. En risk finns också att behörigheter beställs av personer som inte bör kunna beställa vissa typer av behörigheter. Avsaknaden av rutiner för borttag och periodisk genomgång gör också att det finns en ökad risk för att felaktiga behörigheter ligger kvar.	Medel	Ett projekt pågår för att täcka identifierade brister där: • ett IAM system införs • smarta kort kopplas till de behörigheter som IT-personal har • processer för beställning och avbeställning av behörigheter införs. Här ingår också att ”städa” gamla behörigheter så att de informella processerna kan elimineras. I arbetet ingår också att besluta om en ny definition av höga it-behörigheter som finns idag. Idag är definitionen väl vid. Projektet kommer vara avslutat och infört under 2014.

5.10 Status vid revisionens genomförande 1-2 dec 2014:

(I rapport 2014 från Transcendent har denna iakttagelse nummer 5.9)

IAM-systemet med behörighetsprocess kommer att införas successivt från slutet av 2014 och framåt. I och med projektet ska man möta Försäkringskassans regelverk som säger att alla användarkonton ska vara kopplade till inloggning med smarta kort, något som idag inte är fallet för användare med vissa höga behörigheter.

Ett arbete pågår med att implementera ett IAM-system för ökad kontroll av behörighetshantering vilket är under succesiv implementering från slutet av 2014. Detta är något som också kommer tvinga till en fullständig implementering av smarta kort för åtkomst, men även ska möta de säkerhetskrav som Försäkringskassan fastställt för åtkomstkontroll.

Vi rekommenderar att Försäkringskassan säkerställer att detta arbete fortlöper enligt plan och även inkluderar identifiering och specificering av vilka behörigheter som ska hanteras av IT respektive Behörighetsadministration.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.11	Mindre brister i hantering av SID-behörigheter.	I och med att kontrollen av att rätt person beställt SID-behörigheten är manuell, finns en ökad risk för att det begås ett misstag eller att kontrollen glöms bort.	Låg	Funktionalitet som kontrollerar behörig beställare enligt rekommendationen 5.11.3. är implementerad i BOA sedan Q1 2014. Iakttagelsen är åtgärdad.

5.11 Status vid revisionens genomförande 1-2 dec 2014:

(I rapport 2014 från Transcendent har denna iakttagelse nummer 5.10)

Vid upplägg av en ny SID-behörighet genomfördes under början av 2014 en manuell kontroll av att den som har lagt beställningen av behörigheten var en så kallad SID-chef på myndigheten. Sedan februari 2014 så har en automatisk kontroll implementerats i BOA där endast anställd som innehar yrkesrollen SID-chef har möjlighet att beställa SID-behörigheter för anställda på tillhörande kontor.

Vi rekommenderar att man fortsätter med den automatiska kontrollen i BOA för tilldelning av SID-behörigheter. Då felaktig SID-behörighet eller beställning kan ge konsekvenser för enskild person rekommenderar vi Försäkringskassan att hantera felaktig och obehörig beställning av SID-behörighet som en säkerhetsincident.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.12	Brister i uppföljning efter periodisk genomgång av behörigheter.	Att inga återkopplingskrav finns på chefer efter periodiska behörighetsgenomgångar ökar risken för att genomgångarna inte genomförs eller genomförs på fel sätt. Att cheferna inte genomför genomgången 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.	Låg	Idag ställs inga krav på att Behörighetsadministrationen ska kontrollera att cheferna genomför den årliga behörighetsuppföljningen. Dock sker stickprovskontroller av Säkerhetsstaben på årsbasis. Möjligheterna att införa en rutin enligt rekommendationen 5.12.3 kommer att diskuteras med normerande funktion (Säkerhetsstaben) under Q2 2014. Ett nytt behörighetsutdrag är framtaget med anledning av rekommendationen att förtydliga utskicken för behörighetskontroll.

5.12 Status vid revisionens genomförande 1-2 dec 2014:

(I rapport 2014 från Transcendent har denna iakttagelse nummer 5.11)

Vi rekommenderar Försäkringskassan att titta på möjligheterna att införa en rutin för återkoppling efter genomförd periodisk genomgång, för att säkerställa att samtliga chefer gjort kontrollen. Detta skulle även ge möjlighet till sammanställning av statistik rörande hur effektiv processen för behörighetstilldelning och behörighetsförändringar är. Vidare rekommenderar vi Försäkringskassan att förtydliga utskick för kontroll så att granskande chefer lättare kan tolka de tilldelade behörigheterna, de uppges fortfarande vara svårtolkade.

Nr	Iakttagelse	Risk	Risknivå	Försäkringskassans svar till Riksrevisionen 2014-05-16 dnr 017721-2014
5.13	Brister i regelbunden uppföljning av särskild, priviligierad behörighet.	Att periodiska behörighetsgenomgångar inte generellt genomförs för särskilda, priviligierade (höga) behörigheter 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.	Medel	Ett projekt pågår för att täcka identifierade brister där: • ett IAM system införs • smarta kort kopplas till de behörigheter som IT-personal har • processer för beställning och avbeställning av behörigheter införs. Här ingår också att ”städa” gamla behörigheter så att de informella processerna kan elimineras. I arbetet ingår också att besluta om en ny definition av höga it-behörigheter som finns idag. Idag är definitionen väl vid. Även periodiciteten för behörighetsgenomgångar ska fastställas. Projektet kommer vara avslutat och infört under 2014.

5.13 Status vid revisionens genomförande 1-2 dec 2014:

(I rapport 2014 från Transcendent har denna iakttagelse nummer 5.12)

Se även punkt 5.10 ovan. Vi rekommenderar fortsatt Försäkringskassan att säkerställa periodiska behörighetsgenomgångar för särskilda, priviligierade behörigheter inom IT.