Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.2	Systemgenererade listor över applikationsförändringar 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	En systemgenererad lista garanterar **inte** att icke godkända applikationsförändringar produktionssätts. Det borde finnas andra mer preventiva kontroller i flödet som bättre kan säkerställa att det är just **godkända** och **testade** programförändringar som produktionssätts. Försäkringskassan bör säkerställa att endast godkända applikationsförändringar produktionssätts genom att införa tillämpliga nyckelkontroller i sina flöden. Pensionsmyndigheten avser att följa upp status vid den kommande tertialuppföljningen med Försäkringskassan.

4.2 Status vid revisionens genomförande 1-2 dec 2014
Försäkringskassan utreder även möjligheten att använda logglistor från de releasepaket som används vid implementering av förändringar i produktionsmiljön. Lösningen är ej helt implementerad och beräknas kunna börja användas fullt ut från årsskiftet 2014/2015.

Vi rekommenderar att Pensionsmyndigheten verkar för att Försäkringskassan säkerställer att implementering av funktionalitet för att kunna utläsa vilka driftsatta applikationsförändringar som skett i myndighetens kritiska system. Viktigt är att funktionaliteten utformas på sådant sätt att den inte går att kringgå, dvs. att samtliga driftsättningar automatiskt registreras och ej kan manipuleras i efterhand.

Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.3	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	Pensionsmyndigheten delar bedömningen och beskrivningen av risken och rekommenderar Försäkringskassan att se över ändringsrutinerna samt säkerställa ”segregation of duties” vad avser utveckling och test. Pensionsmyndigheten avser att följa upp status vid den kommande tertialuppföljningen med Försäkringskassan.

4.3 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 fortsatt att Pensionsmyndigheten verkar för att Försäkringskassan 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	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.4	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	Pensionsmyndigheten delar bedömningen och beskrivningen av risken och rekommenderar Försäkringskassan att: • tydligare beskriva de olika testnivåerna med bakgrund till vad som ska testas. • tydliggöra hur varje testnivå ska godkännas för att säkerställa att applikationsförändringar är tillräckligt testade innan de produktionssätts. Pensionsmyndigheten avser att följa upp status vid den kommande tertialuppföljningen med Försäkringskassan.

4.4 Status vid revisionens genomförande 1-2 dec 2014

Under 2014 har Försäkringskassan uppdaterat sina testriktlinjer för att få dem mer lättarbetade.

Vi rekommenderar att Pensionsmyndigheten fortsatt verkar för att Försäkringskassan dokumenterar nödvändiga testnivåer för olika typer av ändringar alternativt annat stöd för beslut om nödvändiga testnivåer.

Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.5	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)	Pensionsmyndigheten delar bedömningen och beskrivningen av risken och rekommenderar att Försäkringskassan har rutiner för hur testfall och testdokumentation ska upprättas och sparas samt tillse att rutinen följs. Pensionsmyndigheten avser att följa upp status vid den kommande tertialuppföljningen med Försäkringskassan.

4.5 Status vid revisionens genomförande 1-2 dec 2014

För 11 av 30 testade förändringarna har vi dock 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 Pensionsmyndigheten verkar för 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	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.6	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	Pensionsmyndigheten delar bedömningen och beskrivningen av risken. Dock har vi redan tidigare verkat för att Försäkringskassan utvecklar funktionaliteten i BOA, men utan framgång. Försäkringskassan har då delat bilden av bristerna, men kostnaden för den nödvändiga utvecklingen prioriterades inte. Bland annat av detta skäl har Pensionsmyndigheten själva under 2013 först bedrivit en förstudie och nu under 2014 pågår uppstart av projekt för att införa ett eget centralt IT-stöd som kommer att innehålla den funktionalitet som saknas i BOA. Detta väntas infört under 2015.

4.6 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 Pensionsmyndigheten verkar för 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 att Pensionsmyndigheten verkar för att Försäkringskassan utreder vilka kombinerade behörighetskombinationer i förmånssystemens befintliga roller och profiler som ej är tillåtna enligt givna beslut och riktlinjer för informationssäkerhet.

Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.7	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)	Pensionsmyndigheten anser att det är särskilt viktigt att Försäkringskassan genomför säkerhetsprövning för personal med höga IT-behörigheter, vilket också kravställs i dokumentet *Vägledande principer för samarbete mellan FK och PM v2.0*. Pensionsmyndigheten lägger själva ner ett stort arbete att säkerställa att den personal som har åtkomst till de system som Pensionsmyndigheten själva administrerar är säkerhetsprövade. Pensionsmyndigheten kommer att följa upp mot Försäkringskassan och begära löpande rapportering av status i frågan.

4.7 Status vid revisionens genomförande 1-2 dec 2014

Detta har genomförts enligt intervjusvar.

Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.8	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	Pensionsmyndigheten är med i det arbete (styrgrupp) som i dag genomförs på Försäkringskassan för att åtgärda dokumenterade iakttagelser. 2011 skickade Pensionsmyndigheten ett beställningsunderlag, även kallad BUL (nr 234), med syfte att säkerställa att Försäkringskassan i sin leverans av IT-tjänster svarar upp mot Pensionsmyndighetens krav på rutiner för behörighetsadministration för systemadministratörer. I början av 2013 erhöll Pensionsmyndigheten svar. Där framgick att ett antal förbättringsåtgärder kommer att genomföras. Men det framgick även att tills det att projektet har realiserat en lösning kommer Försäkringskassans IT-avdelning att införa manuella processer för att hantera behörigheter så att hanteringen blir homogen inom de olika teknikområdena. Med bakgrund av Riksrevisionens iakttagelse verkar de manuella rutinerna inte vara helt till fylles. Pensionsmyndighetens nyckelkontroller för teknik- och systemadministrativa behörigheter bör tillämpas för Försäkringskassan. Pensionsmyndigheten kommer att följa upp mot Försäkringskassan och begära löpande rapportering av status i frågan.
4.8 Status vid revisionens genomförande 1-2 dec 2014 (I rapport 2014 från Transcendent har denna iakttagelse nummer 4.7)				

Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
Forts pkt 4.8 Ett arbete pågår med att implementera ett s.k. IAM-system[1] 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 Pensionsmyndigheten verkar för 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.				

[1] IAM = Identity and Access Management

Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.9	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	Enligt Försäkringskassan ska det sedan Q1 i år finnas funktioner i BOA för att kontrollera behörig beställare.

4.9 Status vid revisionens genomförande 1-2 dec 2014

(I rapport 2014 från Transcendent har denna iakttagelse nummer 4.8)

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. I och med att kontrollen av att rätt person beställt SID-behörigheten var manuell under januari 2014, finns en ökad risk för att det begåtts misstag eller att kontrollen glömts bort innan den automatiska kontrollen infördes i BOA under februari 2014.

Vi rekommenderar att Pensionsmyndigheten verkar för att Försäkringskassan 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	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.10	Brister i periodisk genomgång av behörigheter	Att regelbundna genomgångar inte genomförs ökar risken för att behörigheter som bör tas bort finns kvar. Detta ökar i sin tur bland annat risken för att personer som slutat inom Försäkringskassan fortsatt innehar känsliga behörighetskombinationer.	Låg	Pensionsmyndigheten genomför två gånger per år genomgångar av höga IT-behörigheter. I dokumentet *Vägledande principer för samarbete mellan FK och PM v2.0* framgår det att säkerhetsåtgärder ska följa Pensionsmyndighetens interna regelverk för säkerhet om inget annat har överenskommit. Detta innebär att även Försäkringskassan ska genomföra uppföljning av behörigheter två gånger per år för att säkerställa att behörigheter som inte behövs tas bort. Pensionsmyndigheten kommer att begära kontinuerlig statusrapportering av Försäkringskassan. Pensionsmyndigheten anser att risknivån bör klassas om från Låg till Medel.
4.10 Status vid revisionens genomförande 1-2 dec 2014 Denna ryms i iakttagelse 4.8 ovan (punkt 4.7 för 2014).				

Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.11	Avsaknad av skriftlig överenskommelse med Försäkringskassan för hantering av höga IT-behörigheter (2013) Avsaknad av detaljerade krav med Försäkringskassan för hantering av höga IT-behörigheter (2014)	Utan formaliserade krav på tjänster och system ökar risken för att Försäkringskassan inte lever upp till de förväntningar och krav som Pensionsmyndigheten har. Vidare kan detta innebära att uppföljning av efterlevnad inte fullständigt kan genomföras då kraven inte finns dokumenterade.	Medel	Sedan myndighetens start har interna diskussioner förts om hur Pensionsmyndigheten kan få en bättre samverkan inom IT-säkerhetsområdet med Försäkringskassan. Detta har även tydliggjorts efter olika revisionsrapportrar där ett antal förbättringsområden inom säkerhetsområdet har identifierats i samarbetet mellan Försäkringskassan och Pensionsmyndigheten. Med bakgrund till det har Pensionsmyndigheten lagt en beställning om ett samverkansforum mellan Försäkringskassan och Pensionsmyndigheten. Ett huvudsyfte för detta samverkansforum borde initialt vara att ta fram en skriftlig överenskommelse för hantering av höga IT-behörigheter. När dokumentet är fastställt bör forumet sedan användas för att följa upp det som överenskommit.

4.11 Status vid revisionens genomförande 1-2 dec 2014

(I rapport 2014 från Transcendent har denna iakttagelse nummer 4.9)

Under 2014 har ett mer strukturerat samarbete mellan Pensionsmyndigheten och Försäkringskassan utarbetats i form av Samverkansmöten där organisationerna diskuterar områden där samarbete och samkoordinering kan förbättras. Under 2014 har två möten genomförts med ambitionen att ha detta mer regelbundet under 2015.
Vi rekommenderar Pensionsmyndigheten att säkerställa att krav för tjänster och system som handhas av externa parter arbetas fram och avtalas, i detta fall Försäkringskassan och hantering av höga IT-behörigheter. Vidare rekommenderar vi Pensionsmyndigheten att fortsätta med Samverkansmöten tillsammans med Försäkringskassan. Viss formalia bör införas med dokumenterade protokoll eller formella mötesanteckningar för att öka spårbarheten och undvika eventuella missförstånd mellan organisationerna.

Nr	Iakttagelse	Risk	Risknivå	Pensionsmyndighetens svar till Riksrevisionen 2014-05-03, dnr VER 2014-132
4.12	Avsaknad kontroll av genomförd säkerhetsutbildning	Avsaknad av regelbundna informationssäkerhetsutbildningar innebär risk för att för verksamheten känslig och kritisk information behandlas p ett icke tillfredsställande sätt ur ett säkerhetsperspektiv, vilket kan resultera i att informationen kommer obehörig part till handa.	Låg	Pensionsmyndigheten delar bedömningen och rekommendationen och kommer att se över hur vi kan säkerställa detta bättre framöver. Lansering av ny rutin bör kunna ske 2014 Q4.

4.12 Status vid revisionens genomförande 1-2 dec 2014

(I rapport 2014 från Transcendent har denna iakttagelse nummer 4.10)

Pensionsmyndigheten är i färd med att utforma introduktionsutbildningar för anställda och chefer där säkerhet ingår. Dock är formen för dessa inte helt färdigställda men uppskattar att dessa kommer att börja hållas under 2015.

Vi rekommenderar att Pensionsmyndigheten säkerställer och dokumenterar att samtliga medarbetare utbildas inom informationssäkerhet regelbundet. Vidare rekommenderar vi att myndigheten inför en kontroll att personal som tilldelas behörighet i applikationer och system har genomgått aktuell och erforderlig säkerhetsutbildning, så att det vid var tid avspeglar gällande informationssäkerhetskrav.