transcendent group GOVERNANCE RISK COMPLIANCE

IT-revision vid Pensionsmyndigheten

Generella IT-kontroller: Hantering av behörigheter och systemförändringar

Riksrevisionen

2014-01-20

Sammanfattning

Riksrevisionen har inom ramen för 2013 års revision av räkenskaper och förvaltning vid Pensionsmyndigheten anlitat Transcendent Group för att utföra en granskning av generella IT-kontroller avseende hantering av behörigheter och systemförändringar vid Pensionsmyndigheten.

Syftet med granskningen har varit att bedöma huruvida hantering av behörigheter och systemförändringar avseende applikationer som används av Pensionsmyndigheten, men som ägs och driftas av Försäkringskassan kopplat till inkomstpensionsprocessen och processer för anslagsfinansierade förmåner på Pensionsmyndigheten, har en ändamålsenlig intern kontroll och säkerhet för att stödja en tillförlitlig finansiell rapportering.

Granskningens syfte har uppnåtts genom:

- Kartläggning av IT-organisationens processer för applikationsförändring och åtkomsthantering gällande förmåns- och utbetalningssystemen
- Identifiering av nyckelkontroller i dessa processer
- Testning av nyckelkontroller

Inom ramen för granskningen har vi enbart tittat på de system som ägs och driftas av Försäkringskassan vilket innebär att kontroller av processerna gjorts i samband med en parallell granskning av Försäkringskassan vid vilken ett antal iakttagelser gjorts.

Granskningen visar att kontrollerna överlag är effektiva. De brister som har identifierats bedöms inte medföra någon väsentlig påverkan på den interna kontrollen, varför den samlade bedömningen är att Riksrevisionen kan förlita sig i stort på de generella IT-kontroller och applikationskontroller som har utvärderats.

Pensionsmyndigheten rekommenderas dock att se över ändringsrutinerna för COBOL-ändringar, främst gällande ansvarsfördelningen kring utveckling och testning. Dessutom rekommenderas att en generell rutin för alla system tas fram som beskriver hur testfall och testdokumentation ska upprättas och sparas.

Pensionsmyndigheten rekommenderas vidare att säkerställa att BOA:s funktionalitet inkluderar spärrar som gör att endast berättigad chef kan beställa behörigheter. Vidare bör Pensionsmyndigheten utreda vilka behörighetskombinationer som ej är tillåtna. Pensionsmyndigheten rekommenderas därutöver att säkerställa att tjänsteöverenskommelser arbetas fram och avtalas för tjänster och system som handhas av Försäkringskassan avseende hantering av höga IT-behörigheter.

2014-01-20

Andreas Ericson
Uppdragsansvarig

Joachim Klasson
Granskare

Innehåll

1 Inledning

1.1 Uppdrag

Granskning av IT-generella kontroller avseende hantering av behörigheter och systemförändringar kopplat till inkomstpensionsprocessen och processer för anslagsfinansierade förmåner på Pensionsmyndigheten. Uppdraget är ett avrop av Riksrevisionens av ingånget ramavtal (diarienummer Riksrevisionen 38-2011-1507).

1.2 Syfte och omfattning

Syftet med revisionen är att bedöma huruvida hantering av behörigheter och systemförändringar avseende Pensionsmyndighetens applikationer (och därtill hörande databaser och operativsystem) inom inkomstpensionsprocessen och processer för anslagsfinansierade förmåner har en ändamålsenlig intern kontroll och säkerhet för att stödja en tillförlitlig finansiell rapportering.

Granskningen har omfattat följande områden:

- Identifiering av IT-generella kontroller (behörighetshantering och hantering av systemförändringar) för applikationer och därtill hörande databaser och operativsystem

1.3 Avgränsningar

Målet med denna granskning har varit att säkerställa kvalitet i organisationens processer för förändringar av IT-system och hantering av IT-behörigheter. I granskningen har inte alla Pensionsmyndighetens system kontrollerats då Riksrevisionen endast ålagt Transcendent Group att granska de förmånssystem som ägs och driftas av Försäkringskassan men dagligdags används av Pensionsmyndighetens handläggare.

Följande förmånssystem används av Pensionsmyndigheten men ägs och driftas av Försäkringskassan:

- Ålderspension (ÅP37/ÅP38)
  Allmänna pensionen bestående av inkomstpension, premiepension, garantipension samt en tilläggspension[1]. Pensionen finns idag i två utformningar: för personer födda 1937 eller tidigare (ÅP37), respektive 1938 eller senare (ÅP38).
- Efterlevandepension (EP)
  Pension till efterlevande familjemedlem, make/make eller barn, vid dödsfall av make/maka respektive en eller två föräldrar.

[1] Tilläggspensionen kan fås av personer födda mellan 1938-1953. Om du är född 1937 och tidigare består den allmänna pensionen av tilläggspension och garantipension.

- Bostadstillägg till pensionärer (BTP)
  Ett tillägg på pensionen som bidrar till att täcka bostadskostnaden för pensionärer med låg inkomst.
- Särskilt pensionstillägg (SPT)
  Pensionstillägg som kan sökas av personer som under en längre tid avstått från förvärvsarbete på grund av vård av sjukt eller handikappat barn.

Vår granskning de två områdena processerna för förändringshantering samt behörighetshantering har baserats på intervjuer och stickprov[2]. Denna omfattning är i sig inte tillräcklig för att identifiera samtliga risker som kan förekomma i myndighetens processer. Granskningens omfattning syftar till att vi med rimlig säkerhet ska kunna identifiera de mest kritiska riskerna kopplat till nyckelkontrollerna.

Transcendent Group har parallellt med denna granskning genomför en motsvarande granskning vid Försäkringskassan vilket skapar ytterligare förståelse för det samarbete som finns myndigheterna emellan.

1.1.1 Applikationsförändringar

En process för applikationsförändring kan ibland innehålla ett stort antal kontroller av varierande karaktär. Testfasen i denna granskning har avgränsats till att endast beakta de kontroller som bedömts vara mest signifikanta för att minska risken för felaktiga applikationsförändringar i Pensionsmyndighetens IT-system.

Inom ramen för denna granskning har vi inte beaktat hur Försäkringskassans och Pensionsmyndighetens processer till beslut om projekt, eller hur verksamheterna bidrar till styrning av projekt i myndigheternas utvecklingsplaner.

1.1.2 Åtkomsthantering

Även åtkomsthantering kan innefatta ett stort antal kontroller. Vi har under denna testning fokuserat på tillägg och borttag av behörigheter samt periodiska genomgångar av behörigheter i system. Detta för att kunna bedöma att risken för obehörigas tillgång till IT-systemen är så liten som möjligt.

1.4 Metod

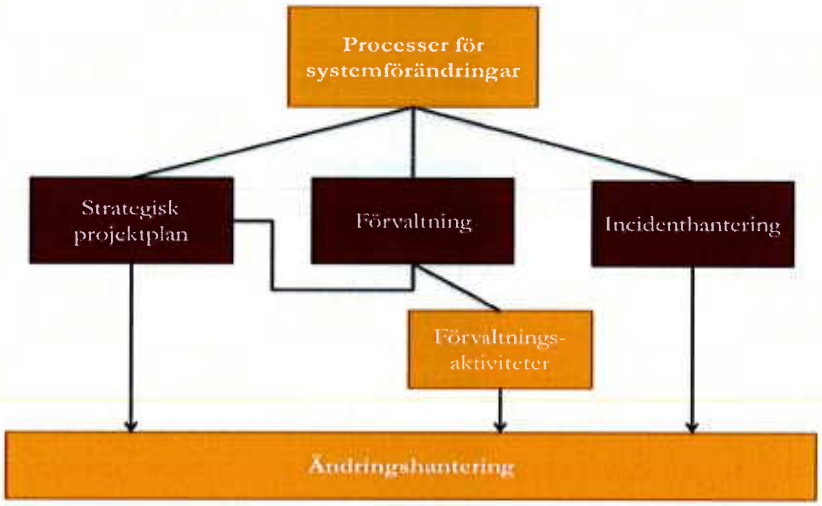
Granskningen har utförts i enlighet med överenskommen uppdragsbeskrivning. För information om metod och vilka personer som intervjuats inom ramen för granskningen; se bilaga 1.

[2] Stickprov baseras på ett slumpmässigt urval från perioden mellan 2013-01-01 och 2013-10-23 för systemförändringar samt från perioden mellan 2013-01-01 och 2012-11-26 för hantering av behörigheter.

2 Granskning av processer för systemförändringar

2.1 Beskrivning av processen för systemändringar

Systemförändringar vid Pensionsmyndigheten hanteras olika beroende på om det avser en planerad ändring eller en rättning till följd av en akut incident. Vidare finns vissa skillnader i hanteringen beroende på om det är en stor förändring som är resurskrävande eller en mindre ändring.



Figur 1 Systemförändringar

Applikationsutveckling sker både i förvaltningsorganisationen och i projektform. Myndigheten har en strategisk plan som innehåller den planerade utveckling som ligger utanför förvaltningsplanen och akuta incidenter (se avsnitt 2.2). Utvecklingen av ny funktionalitet styrs således av den strategiska planen medan planerat underhåll av applikationerna styrs av förvaltningsplanen. Objektägarna ansvarar för hantering av både projektportföljen och förvaltningsportföljen. Strategiska projekt och planerade förvaltningsprojekt ingår i en gemensam utvecklingsplan för Pensionsmyndigheten och Försäkringskassan och överses av en gemensam styrgrupp kallad *Styrgrupp Projektportfölj*. Utöver detta kommer löpande utvecklings-, förbättrings- och förändringsförslag från andra instanser i myndigheten som efter utvärdering kan införas i projektportföljen, men som i huvudsak hanteras i förvaltningsplanen. Parallellt med den strategiska projektplanen och förvaltningsplanen finns en ITIL[3]-baserad process för hantering av incidenter och fel i drift och förvaltning.

[3] IT Infrastructure Library, består av en serie publikationer som ger stöd för kvalitativa IT-tjänster samt de processer och faciliteter som behövs för att stödja dem.

För mer information om Pensionsmyndighetens olika applikationsförändringsprocesser, se kommande avsnitt:

- Strategisk projektplan, avsnitt 3.2
- Förvaltningsplan, avsnitt 3.2
- Ändringshantering, avsnitt 3.4

2.2 Strategisk projektplan

Vid en årlig verksamhetsplanering diskuteras förslag på utveckling som ska ske under året, dels hos Pensionsmyndigheten men även gemensamma projekt Pensionsmyndigheten och Försäkringskassan emellan. Dessa prioriteras och planeras eventuellt in i den strategiska projektplan som finns för Pensionsmyndighetens utvecklingsuppdrag. Annan input till den strategiska projektplanen kan vara att myndigheternas uppdrag ändras eller lagändringar som planeras eller redan finns beslutade. Från förvaltningsprocessen kan större utvecklingsuppdrag komma om bedömning har gjorts att utvecklingen ska bedrivas som projekt och hanteras inom den strategiska projektplanen (se avsnitt 2.3).

För att utveckling vid Pensionsmyndigheten ska drivas inom den strategiska projektplanen ska ett eller flera av följande kriterier vara uppfyllda:

- Att Generaldirektören av någon anledning vill följa och bevaka
- utvecklingen på grund av att projektet är av särskild strategisk betydelse
- Att utvecklingen är komplex eller har kritiska beroenden
- Att utvecklingen påverkar eller involverar flera delar av myndigheten
- Att utvecklingen är tvingande, exempelvis av juridiska skäl
- Att utvecklingen har en uppskattad kostnad som överstiger 500 000 SEK

2.2.1 Styrning av projekt

När beslut fattats om att ett utvecklingsuppdrag ska drivas som projekt finns en tydlig struktur för hur uppdraget ska bedrivas. För detta använder sig Pensionsmyndigheten av projektstyrningsmodellen Pejl. Modellen utgör en process från myndighetens behov och strategier till hemtagningen och uppföljningen av effekterna efter projektavslut. Beslutspunkter, status samt utveckling i arbetet ska löpande följas upp i förhållande till projektets mål, tidsplan och budget. Likaså ska riskhantering följas upp regelbundet. Modellen innehåller fasta beslutspunkter och processteg som beskriver vad projektet ska göra.

Uppföljning och kontinuerlig kontroll sker av projekt som ingår i projektportföljen genom:

- Att följa projektens veckovisa statusrapportering
- Att månadsvis följa upp ekonomiskt utfall
- Att genomföra löpande avstämning med IT-tjänsteleveranser

- Att genomföra återkommande uppföljningsmöten med projektledarna
- Att kvalitetssäkra projektdokumentation och se till att obligatoriskt projektunderlag existerar och kontrolleras
- Att regelbundet kommunicera med IT-beredning angående den övergripande planeringen. Det säkerställer projektportföljens genomförande samt flaggar för om omprioriteringar behöver övervägas och genomföras
- Att minst en gång per kvartal hålla möten där projektledarna för de uppdrag som ligger i projektportföljen kan träffas och utbyta information och diskutera aktuella problem eller möjligheter
- Att en gång per månad summera status och ekonomiskt utfall som gäller hela projektportföljen såväl som för varje enskilt projekt i en månadsrapport
- Att ta fram en relevant agenda och att vara föredragande på styrgruppsmöten för projektportföljen
- Att vid behov av omprioriteringar eller andra beslut om förändringar av projektportföljen ta fram beslutsunderlag och åtgärder
- Att tillhandahålla en övergripande projektportföljsbeskrivning som uppdateras löpande
- Att följa upp effekthemtagning av uppdragen i projektportföljen

2.3 Förvaltningsplan

Pensionsmyndigheten använder sig av modellen pm³ för förvaltningsstyrning. Modellens grundtanke är att förvaltningen delar in ägarskap och underhåll efter objekt istället för enskilda system. Myndigheten använder modellen som stöd vid strukturering av förvaltningsverksamhet och fastställer bl.a. ansvarsroller och uppföljning för en organisations samtliga förvaltningsobjekt.

För varje förvaltningsobjekt inom Pensionsmyndigheten finns en förvaltningsledning som består av två så kallade objektägare som i regel utgörs av organisationens linjechefer (verksamhetens och IT:s representanter) samt förvaltningsledare för IT samt verksamheten. Förvaltningsledningen ansvarar för uppföljning och utveckling inom sitt objekt. För varje år med start 1 januari ansvarar objektägarna för att, i samråd med förvaltningsledningen, ta fram en förvaltningsplan för sitt objekt. Varje plan tar upp verksamhetsnära förvaltning samt IT-nära förvaltning inom respektive objekt och består främst av mindre vidareutvecklingsprojekt och vidmakthållanden. De olika förvaltningsplanerna samlas sedan i en myndighetsgemensam förvaltningsportfölj.

För förvaltningsaktiviteter som återfinns i förvaltningsplanen och uppskattas överstiga 1-1,5 MSEK utförs en utvärdering om genomförandet istället ska ske som ett strategiskt projekt. Vid behov kan även utvecklingsuppdrag med lägre kostnad bedrivas som projekt. Beslut ska då fattas att projektet ska ingå i den strategiska projektportföljen, vilket görs av Generaldirektör efter föredragning i styrgruppen för projektportföljen (se avsnitt 3.2). Om ett utvecklingsförslag skulle få avslag om att drivas i projektform, finns följande fortsättningssteg:

Att utvecklingen drivs som en förvaltningsaktivitet om utrymme finns i budgeten.

- Att utvecklingen drivs som ett avdelningsinternt projekt inom förvaltningen.
- Att utvecklingen nedprioriteras och genomförs vid en senare tidspunkt.
- Att utvecklingen avslås.

2.3.1 Styrning inom förvaltningsprocessen

Förvaltningsledningen ansvarar för beslut beträffande förslag till förvaltningsplan, prioritering och planering inom ramen för förvaltningsplanen, uppföljning av utfall mot förvaltningsplanen samt beredning av beslutsunderlag inför styrgruppen. Vid behov är även andra operativa roller med vid beslutsfattande. Gruppen sammanträder 1-2 gånger per månad på initiativ från förvaltningsledarna.

Styrgrupp Förvaltningsobjekt ansvarar för att godkänna den årliga förvaltningsplanerna och dess budget samt beslut om utökning eller indragning av resurser. Nyligen har ett beslut tagits att sammanföra de två objektsfamiljerna man tidigare haft till en gemensam styrgrupp, det vill säga Styrgrupp Förvaltningsobjekt.

I OF-styrgruppen ingår objektägare från verksamheten och IT för de ingående objekten. Föredragande är förvaltningsledare från verksamheten och IT. OF-styrgruppen sammanträder minst månadsvis, dock mer frekvent vid behov.

Utöver ovan nämnda beslutsforum håller varje objekt månadsvisa möten mellan objektägare och förvaltningsledare från verksamheten och IT. Syftet med dessa möten är att följa objektets status och att förbereda eventuella frågor som ska tas upp i objektfamiljsstyrgruppen. Samtliga förvaltningsledare samlas var tredje vecka och diskuterar samordning, arbetssätt, kontaktvägar och gränsdragningar.

2.4 Ändringshantering

Vid Pensionsmyndigheten finns fyra möjliga sätt att implementera en förändring:

- Stora releaser
- Små releaser
- Servicefönster
- Akuta ändringar

Dessa fyra kategorier beskrivs mer ingående i detta avsnitt.

2.4.1 Stora releaser

En stor release innebär ett planerat tillfälle där både förvaltningsdrivna ändringar och ändringar som tillhör den strategiska projektportföljen kan ingå. En releaseansvarig ansvarar för en releaseplan och koordinerar de utvecklingsuppdrag som ska ingå i releasen. Stora releaser är inplanerade tre till fyra gånger per år och infaller oftast i februari, maj, september samt november. Historiskt sett har dock en till två av dessa tillfällen klassats som små, då ändringarna inte varit av omfattningen motsvarande en stor

release. En stor release innefattar generellt ändringar som berör de stora kärnsystemen som i sin tur integrerar med andra system. Vid dessa releaser ligger därför stort fokus på test och acceptanstest samt en tydlig styrning och kontroll innan driftsättning.

Stora releaser är samordnade mellan Försäkringskassan och Pensionsmyndigheten. I praktiken är det enbart vid de stora releaserna som Pensionsmyndigheten produktionssätter förändringar i något av de system som driftas av Försäkringskassan, och därmed ingår i denna granskning. Utöver detta kan Försäkringskassan genomföra små releaser där Pensionsmyndigheten kan ha ett beroende. Releaseansvarig har därför kontakt med sin motsvarighet vid Försäkringskassan. Tillsammans med denna planeras hålltider för test och leveranser. Se kapitel 2.5 för mer information om avtalsförhållanden mellan Pensionsmyndigheten och Försäkringskassan.

2.4.2 Små releaser

Små releaser berör främst de system som ägs och driftas av Pensionsmyndigheten själva. Detta eftersom ändringar i övriga system måste gå i de myndighetsöverskridande stora releaserna. Dessa releaser består oftast av ändringar som är inplanerade i förvaltningsplanen. Oftast har en förvaltningsledare inom IT det övergripande ansvaret för releasen men det kan variera beroende på vilka system och objekt som berörs. När ändringen är redo för produktionssättning överlämnas releasen till Change Manager som ansvarar för att ändringen drivs i mål och att berörda parter är informerade.

2.4.3 Servicefönster

Produktionssättning av IT-relaterade infrastrukturförändringar sker i så kallade servicefönster. Dessa genomförs regelbundet cirka två gånger per månad, samt genom löpande produktionssättningar när ändringarna är av enklare karaktär. När ett servicefönster äger rum planeras ändringarna in under en vecka i följd, inklusive helg. Ofta genomförs ändringarna dagtid, men standardändringar kan även förberedas och implementeras under natten. Pensionsmyndighetens Change Manager är ansvarig även för produktionssättningen som äger rum inom ramen för servicefönster.

2.4.4 Akuta ändringar

Akuta ändringar är ändringar som behöver genomföras omgående eller inom en snar framtid och därmed hamnar utanför ramen för en release. Incidenter inträffar i princip dagligen och rapporteras in via Helpdesk hos Försäkringskassan som registrerar ärendet i verktyget ARS[4] eftersom Pensionsmyndigheten köper supporttjänster av Försäkringskassan. Tillhör ärendet Pensionsmyndigheten går det sedan vidare till och registreras i Pensionsmyndighetens ärendehanteringssystem RT[5]. RT samlar även alla automatgenererade larm och driftstörningar fångas på så sätt upp direkt. Myndighetens incidentmanager och drift bevakar RT dygnet runt. Incidentmanager är ansvarig för att

[4] Försäkringskassan använder verktyget ARS för stöd och spårbarhet i utförandet av ITIL-processer.
[5] Request Tracker.

hantera akuta fel som uppstår. Om behov finns för ändring i produktion registreras ärendet i SBM [6]och Change Manager involveras.

De flesta större incidenter som inträffar är dock fel som uppstått vid en release. Åtgärder för incidenter som ej bedöms vara akuta inom de system som driftas av Försäkringskassan produktionssätts inte förrän vid nästa stora release. Vid akuta incidenter som påverkar funktionaliteten av Pensionsmyndighetens system stängs systemet ned för en akutåtgärd.

2.5 Avtalsförhållanden med Försäkringskassan

Pensionsmyndigheten bildades 2010 efter en sammanslagning av tidigare PPM och delar av Försäkringskassan. Detta har lett till att Försäkringskassan idag äger och driftar några av de applikationer som Pensionsmyndighetens handläggare använder sig av. För Försäkringskassans IT -organisation betraktas Försäkringskassans och Pensionsmyndighetens verksamheter som jämförliga beställarorganisationer, men för att reglera denna relation har en överenskommelse[7] upprättats beträffande rutiner för beställning av förstudie- och genomförandeuppdrag som baseras på Pensionsmyndighetens utvecklingsbehov.

Inför varje verksamhetsår planerar Pensionsmyndighetens Projektkontor vilka utvecklingsprojekt som ska bedrivas på tre års sikt och inför det i ett förslag till reviderad utvecklingsplan[8]. Underlaget diskuteras vid ett myndighetsgemensamt möte varefter Pensionsmyndighetens och Försäkringskassans generaldirektörer beslutar om införande i den gemensamma utvecklingsplanen. Utvecklingsplanen, som består av både planerade och pågående uppdrag, revideras av båda myndigheterna tre gånger per år[9] enligt samma rutin som ovanstående.

Vid beställning av projektuppdrag från Försäkringskassan inleds processen med ett presentationsmöte där förslaget presenteras och diskuteras myndigheterna emellan. Detta görs för att:

- säkerställa att Försäkringskassan har kapacitet att genomföra förändringen
- se om även Försäkringskassan kan ha nytta av förändringen
- kontrollera om förändringen kommer att påverka Försäkringskassans system

[6] IBM Service Manager for Smart Business.
[7] Beskrivs i Projekt på Pensionsmyndigheten – Handledning, 2013-10-25.
[8] Beställningar avseende IT-system som både Pensionsmyndigheten och Försäkringskassan nyttjar ska prioriteras av myndigheterna gemensamt.
[9] I mars, maj och september.

Därefter görs en s.k. BUL[10]-beställning som består av fyra moment: Presentation av idé, effektanalys, projektanalys samt ett leverantörskontrakt från Försäkringskassan. Det faktum att en beställning lagts innan beslut om utveckling slutgiltigt tas innebär att förändringen kan påbörjas så fort som beslut[11] tagits att förändringen ska genomföras. Denna process används främst för stora projekt och syftar till att effektivisera samarbetet mellan Pensionsmyndigheten och Försäkringskassan eftersom en resurssäkring för projektet gjorts i och med BUL-beställningen.

För förvaltningsaktiviteter består processen istället enbart av en BUL-förfrågan eller BUL-beställning till Försäkringskassan som avgör om förslaget kan genomföras. Denna förfrågan skickas innan införandet av aktiviteten i förvaltningsplanen. Då Pensionsmyndigheten baserat på svar på BUL-förfrågan fattat beslut om att gå vidare med beredningen och infört aktiviteten i Förvaltningsplanen skickas en beställning på genomförande till Försäkringskassan.

All formell kontakt mellan myndigheterna sker via de tjänsteansvariga. Dock har t.ex. projektledare direktkontakt vid genomförande av uppdrag för att följa upp och diskutera status. Varje månad upprättar Försäkringskassans projektledare uppföljningsunderlag för samtliga uppdrag enligt etablerade rutiner och skickar till Pensionsmyndigheten. Utöver detta upprättar Försäkringskassans utvecklingsstab en myndighetsgemensam statusrapport med budget varje tertial och skickar till Försäkringskassans ekonomistab och Pensionsmyndighetens ledningsstab. Rapporten presenteras också på ett tertialmöte. Försäkringskassans tjänsteansvarig sammanställer verkligt utfall för samtliga projekt och skickar till Pensionsmyndigheten samt till Försäkringskassans ekonomistab som bevakar att utfallet ligger i linje med överenskommen budget. Uppföljningsmöten för detta genomförs regelbundet, minst en gång per månad.

För att säkerställa att Försäkringskassan, medvetet eller av misstag, inte implementerar applikationsförändringar i de system Pensionsmyndigheten använder som Pensionsmyndigheten inte godkänt eller känner till förlitar man sig på de nyckelkontroller inom programförändringsprocessen som Försäkringskassan har. Pensionsmyndigheten har även genomfört ett arbete med att kartlägga vilka personer som har möjlighet att göra applikationsförändringar för att få bättre kontroll. Dessa roller är: Projektbeställaren, Projektledaren och Förvaltningsledare. Detta är även tydliggjort i beställningsformuläret.

2.6 Test av kontroller i applikationsförändringsprocesserna

[10] Förkortning för Beställningsunderlag
[11] Så kallat BP3-beslut

Då de förmånssystem som Pensionsmyndigheten använder i sin handläggning ägs och driftas av Försäkringskassan genomgår de samma process för applikationsförändringar som Försäkringskassans övriga förmånssystem. Av den anledningen har vi valt att testa applikationsförändringsprocessen för Pensionsmyndighetens system i samband med den granskning som parallellt genomförts på Försäkringskassan. För närmare information om processbeskrivningar och tester utförda av nyckelkontroller i processerna hänvisar vi därmed till rapporten: *IT-granskning av IT-revision vid Försäkringskassan – Generella IT-kontroller: Hantering av behörigheter och systemförändringar.*

3 Granskning av processer för behörighetshantering

3.1 Beskrivning av hanteringen av behörigheter

Skyddet av Pensionsmyndighetens informationstillgångar regleras i ett regelverk för informationssäkerhet och föreskrifter angående behandling av personuppgifter. För att konkretisera regelverkets innehåll har Pensionsmyndigheten kompletterat dessa dokument med ett antal riktlinjer. En lista över dessa återfinns i bilaga 1.

BOA är det övergripande verktyg som används hos Försäkringskassan och Pensionsmyndigheten för beställning och administrering av användare och behörigheter till applikationer. Anställda hos Pensionsmyndigheten som i sin yrkesroll använder sig av system som ägs av Försäkringskassan loggar in med ett smart kort, på samma sätt som anställda av Försäkringskassan. Detta inloggningssätt har sedan granskning 2012 införts även för Pensionsmyndighetens interna inloggning till klientdatorer. Numera görs inloggning med smarta kort där samma kort används för anslutning via fjärrskrivbordet till Pensionsmyndighetens system som går i Försäkringskassans miljö. Pensionsmyndighetens behörighetshantering för de applikationer som är med inom ramen för denna granskning sker tillsammans med Försäkringskassan och utförs av Behörighetsadministrationen i Arvidsjaur.

Pensionsmyndigheten räknar med att på sikt sluta använda BOA för beställning och godkännande av behörigheter, där myndighetens inriktning är att man ska ta hem denna funktion som innehåller en beslutsdel och själva behörighetsregistret. Målbilden är därför att skaffa ett internt IAM[12]-stöd som man vid behov integrerar med extern del (läs Försäkringskassan eller annan samarbetspartner).

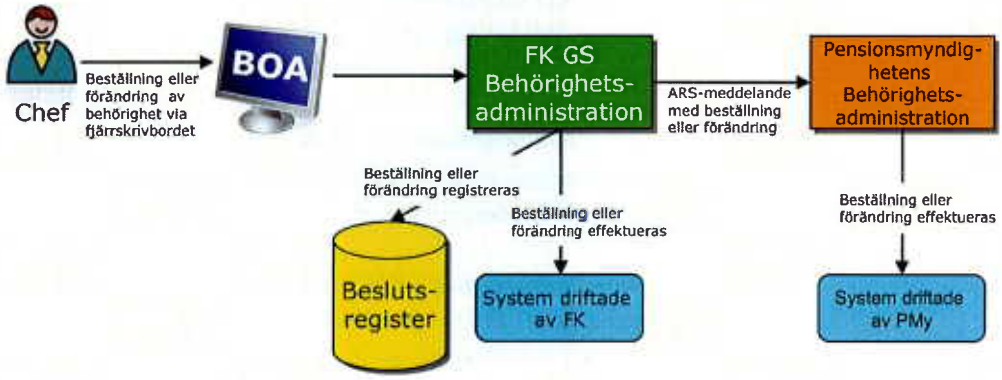
Pensionsmyndigheten har därför inlett ett IAM-projekt som bedrivs internt på Pensionsmyndigheten där man under våren 2013 tagit fram en IAM-strategi, vilken beslutades av generaldirektören under maj 2013. Införandet av ett nytt IAM-system ska täcka både verksamhetsbehörigheter samt IT-behörigheter.

Pensionsmyndigheten har nu nått BP1 för IAM-projektet och förankrat ett behov och inriktning för ett införandeprojekt. Pensionsmyndigheten bedömer att man kan slutföra införandet av en IAM-lösning med stödprocesser under första halvan 2016.

[12] Identity and Access Management. Ett samlingsbegrepp för styrning av resurser rörande identitets- och åtkomsthantering.

3.2 Tilldelning av nya behörigheter

Pensionsmyndigheten har dokumenterade riktlinjer[13] för beställning av nya verksamhetsbehörigheter som är oberoende av system, behörighetstyp och om personen som ska ha behörigheten är intern eller extern. Enligt dessa riktlinjer fylls en fördefinierad elektronisk blankett i av den anställdes närmsta chef eller ansvarig för projekt om en extern person ingår. Enbart dessa personer är behöriga att godkänna nya behörigheter för en anställd. Försöker exempelvis fel chef göra en beställning ska inte ansökan gå igenom. Dock görs ingen automatisk kontroll av detta i BOA, utan kontrolleras mot listor av Behörighetsadministrationen (BA) som en manuell kontroll.



Figur 2 Process för behörighetshantering (bild tillhandahållen av PM)

Vid nyanställning beställer närmaste chef grundbehörighet till den nyanställde vilket innebär tillgång till dator, intranät, mail, portal etc. För att få tillgång till förmånssystemen krävs ytterligare en beställning av behörigheter kopplade till de arbetsuppgifter personen har. För att få behörighet utöver grundbehörighet krävs att man genomgår en säkerhetsutbildning[14]. Det görs dock ingen kontroll av Behörighetsadministrationen innan behörigheterna lagts upp att detta har genomförts.

För konsulter gäller samma process som för en nyanställd. Eftersom konsulterna oftast arbetar i projektroller är det istället projektägaren som är beställare av behörigheterna. Konsulter läggs upp i Active Directory[15] med tidsbegränsning så att behörigheten spärras i enlighet med avtalad tid, vilket leder till automatiskt avaktivering vid datumet för kontraktets slut. För att ha möjlighet att förlänga behörigheten krävs att avtalet förlängts. Behövs utökade behörigheter för att konsulten ska kunna utföra sitt arbete är det närmaste chef eller projektledares ansvar att lägga in en tidsbegränsning för behörigheten i den utökade behörigheten.

[13] Riktlinje – Säkerhet för chefer (2010).
[14] Datorstödd informationssäkerhetsutbildning för användare (DISA) som ges ut av Myndigheten för samhällsskydd och beredskap.
[15] Active Directory (AD) är en katalogtjänst som innehåller information om olika resurser i ett nätverk, t.ex. datorer, skrivare och användare. För att komma åt resurser i Pensionsmyndighetens eller Försäkringskassans nätverk krävs en första inloggning i myndigheternas AD.

Inom både Försäkringskassan och Pensionsmyndigheten finns handläggare med behörighet att handlägga ärenden rörande personer med skyddade personuppgifter, s.k. SID[16]-handläggare. Vilka som är SID-handläggare ska enligt riktlinjerna enbart vara känt av chef på högre nivå och vid Pensionsmyndigheten finns två utpekade så kallade SID-chefer.

En manuell kontroll av SID-beställningar ska alltid göras av Försäkringskassans Behörighetsadministration, där man kontrollerar att det är en behörig SID-chef som gör beställningen. Om behörighet beställs för SID-åtkomst av person som inte är behörig beställare (SID-chef) så är rutinen att Behörighetsadministrationen vid Försäkringskassan ska återkoppla detta direkt till SID-chef via e-post. Dock så hanteras detta inte som en incident, utan det ligger på den SID-chef som man återkopplar till som får bedöma från fall till fall.

Under intervjuer har det framkommit att Pensionsmyndigheten har tidigare påpekat brister för Försäkringskassan som Pensionsmyndigheten anser finns i BOA idag. De funktioner man önskar inkludera är främst:

- **Automatisk begränsning i BOA för behörighetsbeställningar.**
  Det saknas spärrar i behörighetshanteringssystemet BOA för att förhindra att personer beställer behörigheter utöver sin befogenhet. I dagsläget finns endast automatiska begränsningar i BOA gällande att beställande person själv måste inneha behörigheten Chef, samt att personen enbart kan beställa inom sitt behörighetsområde (dvs. kontor[17]). Kontor innebär (byggt enligt försäkringskassans organisationsmodell) att rollen kan administrera samtliga inom det kontoret, exempelvis huvudkontoret. Det innebär inte att personen i fråga nödvändigtvis är närmaste chef och därmed är behörig att beställa för en viss medarbetare.
- **BOA är inte integrerat med alla system**
  BOA är idag inte sammankopplat med alla system som används av Pensionsmyndigheten. Det innebär att man för vissa system måste registrera behörigheten i BOA och manuellt implementera behörigheten i det faktiska systemet.

3.3 Borttagning av behörigheter

För att säkerställa att obehöriga inte har tillgång till Pensionsmyndighetens system eller anställda innehar felaktiga behörigheter måste användarbehörigheter tas bort vid avslutad anställning eller vid byte av arbetsuppgifter inom Pensionsmyndigheten.

3.3.1 Avslutad anställning

[16] Skyddad identitet
[17] En person kan tillhöra behörighetsområde Hela PM, vilket innebär att det inte finns några applikationsbegränsningar för vem han eller hon kan beställa behörigheter till inom organisationen.

Vid meddelande från personalavdelningen om en anställds kommande anställningsavslut läggs slutdatum in i Active Directory då kontot ska inaktiveras. Man tar då även tillbaka passerkort, dator, dosa för fjärrinloggning etcetera från den anställde, vilket innebär att den anställde inte längre har fysisk access till lokalerna eller annan möjlighet att logga in i Active Directory. Utan möjlighet att logga in i Active Directory går det inte heller att komma vidare in i applikationer. Borttag av behörigheter ska även beställas av chef direkt i BOA eller per blankett för system utanför BOA. Sedermera tas även behörigheten bort från systemen inom en 30-dagarsperiod. Detta sker genom en kompenserande kontroll där Behörighetsadministration tar del av lönelistor för Pensionsmyndigheten via Statens Service Center, vilka sedan jämförs med aktuella behörigheter och där man avslutar de som inte finns representerade på lönelistan. Användarkonton sparas därefter i tio år innan de raderas från AD och systemen för att behålla spårbarhet.

Vid intervjuer med Försäkringskassans behörighetsadministration framkom det att det brustit i den månadsvisa kontrollen då lönelistor inte gjorts tillgängliga för Behörighets-administrationen sedan sommaren 2013. Detta var vid granskningens tillfälle noterat av både Pensionsmyndigheten och Försäkringskassan, men man hade inte fortsatt arbetet med att identifierat orsaken för att möjliggöra en lösning på problemet.

3.3.2 Ändrad anställning

Vid en förändrad anställning eller geografisk flytt av en anställd gäller att den anställdes behörigheter ska tas bort av den chef som den anställde lämnar. Enligt gällande riktlinjer[18] är det den före detta chefens ansvar att se till att detta sker. Chefen för den anställdes nya roll får sedan skicka in en beställning för behörigheter på nytt, på samma sätt som för en helt nyanställd medarbetare. Chefen för den anställdes nya roll får sedan skicka in en beställning för behörigheter på nytt, på samma sätt som för en helt nyanställd medarbetare. Detta för att närmsta chef alltid ska vara den som begärt de behörigheter som är aktuella för den innehavda rollen. Vid beställning av nya behörigheter kan den nya chefen se den anställdes existerande behörigheter. Skulle det då finnas kvar gamla behörigheter kan detta uppmärksammas och tas bort innan de nya läggs upp.

Om en chef inte har meddelat förändring av en medarbetares anställning och därmed inte beställt en degradering av behörigheter, samt om kvarvarande behörigheter inte uppmärksammas av den nya chefen finns en risk för att gamla behörigheter ligger kvar fram till den periodiska genomgången.

3.4 Periodisk genomgång av behörigheter

Enligt Pensionsmyndighetens riktlinje *Säkerhet för chefer (2010)* ska en total uppföljning av samtliga användarbehörigheter genomföras en gång per år för vanliga behörigheter för att säkerställa att dessa är behovsanpassade baserat på arbetsuppgifter. Det yttersta ansvaret för att detta utförs ligger på myndighetens säkerhetschef. Vid dessa genomgångar upprättar och distribuerar en behörighetsadministratör listor över de medarbetare som tillhör respektive chefs kostnadsställe som chefen sedan väntas granska. Det är alltid

[18] Riktlinje - Säkerhet för chefer (2010)

närmsta chef som har ansvaret för sina medarbetares behörigheter och att dessa är roll- och behovsanpassade. För projektanställda är det projektägaren som har ansvaret att utföra genomgången och se till att deltagarna har rätt behörigheter. För högre behörigheter är det i riktlinjerna kravställt att en liknande genomgång ska genomföras gång i per halvår.

Inom Pensionsmyndigheten finns en rutin för att årligen säkerställa att samtliga chefer genomfört en genomgång av sina underställda medarbetares behörigheter. Initialt gör *Säkerhet och fastighetsenheten* en avstämning mellan de olika behörighetsregistren:

- BOA – Försäkringskassans system innehållande behörighetsbeställningar och beslut
- PM Active Directory – Pensionsmyndighetens Active Directory innehållande samtliga konton för den administrativa miljön på myndigheten.
- Agresso - lönelistor från Statens Service Center som ses som faktiska anställda vid Pensionsmyndigheten.

Denna kontroll säkerställer att endast anställda (enligt lönesystemet) är befintligt registrerade i Active Directory och BOA. Därefter tas underlagen fram i Excelformat som skickas ut till respektive chef för granskning. I informationen från *Säkerhet och fastighetsenheten* framgår tydligt att samtliga chefer ska returnera de kontrollerade listorna. Listorna ska vara markerade för varje kontrollerad medarbetare. Chefen måste däremot själv kontrollera medarbetarnas behörigheter genom att logga in i BOA. Utöver det registrerar de samtidigt i BOA om det ska ske några förändringar av behörigheterna.

Korrigering av markerade förändringar avseende stängning av konton genomförs inte förrän listan inkommit till *Säkerhet och fastighetsenheten*[19].

De kontroller rörande behörigheter till applikationer som ska genomföras av respektive chef är:

- Utvärdering och uppdatering av behörigheter i BOA.
- Utvärdering och godkännande av användarkonton, d.v.s. personen är fortfarande anställd och aktiv medarbetare.

Vidare har Pensionsmyndigheten en kompenserande detektiv kontroll där Försäkringskassan månatligen går igenom SID-behörigheter och återrapporterar status enligt SLA. Kontrollen avser de SID-behörigheter som är upplagda under föregående månad och att de är beställda av behörig SID-chef. Pensionsmyndigheten verkar för att Försäkringskassan ska bygga systemstöd för den kontrollen som Försäkringskassan sagt att de ska införa. Pensionsmyndigheten uppfattar i sin dialog med Försäkringskassan att de kommer att realisera detta i februarireleasen 2014.

[19] För detaljerad information, se *Rutin för utvärdering av tilldelade behörigheter v1.3*.

3.5 Test av nyckelkontroller

3.5.1 Test av kontroller i åtkomsthanteringsprocessen

Behörighetshanteringen för de system som är inom ramen för denna granskning ligger hos Försäkringskassans Behörighetsadministration. Därav har vi valt att testa behörigheter för de system som Pensionsmyndigheten använder men som ägs och förvaltas av Försäkringskassan i samband med den parallella granskning som genomförts på Försäkringskassan. För närmare information om processbeskrivningar och tester utförda av nyckelkontroller i processerna hänvisar vi därmed till rapporten: *IT-revision vid Försäkringskassan – Generella IT-kontroller: Hantering av behörigheter och systemförändringar.*

Pensionsmyndighetens kontroll av behörigheter genom periodiska genomgångar är en effektivt utformad kontroll som skiljer sig från den kontroll som görs inom Försäkringskassan. 2013 års genomgång har utförts under hösten men var vid granskningstillfället inte färdigställd.

4 Identifierade iakttagelser och förbättringsområden

Baserat på resultatet av genomförd granskning har Transcendent Group identifierat ett antal iakttagelser där vi ser att Pensionsmyndigheten har förbättringsmöjligheter.

De förmånssystem som denna granskning fokuserat på ägs och driftas av Försäkringskassan, vilket innebär att testning av kontroller kring dessa system gjorts inom ramen för en parallell granskningen vid Försäkringskassan. Vissa av de iakttagelser som gjorts vid Försäkringskassan kan således påverka de system som används av Pensionsmyndigheten som fortsatt äger risken. Vi har under genomförda tester identifierat vissa brister i genomförda kontrollaktiviteter.

4.1.1 Riskklassificering

Respektive noterad iakttagelse har riskklassificerats enligt följande skala:

Hög	Hög risk för negativ påverkan på riktighet och/eller fullständighet i finansiell rapportering. Bör åtgärdas omedelbart.
Medel	Medelstor risk för negativ påverkan på riktighet och/eller fullständighet i finansiell rapportering. Bör åtgärdas inom snar framtid.
Låg	Låg risk för negativ påverkan på riktighet och/eller fullständighet i finansiell rapportering. Bör dock åtgärdas på sikt.

Riskbedömningen har gjorts med hänsyn till sannolikhet och påverkan avseende noterad iakttagelse.

4.1.2 Riskklassificering för samtliga identifierade iakttagelser

I följande tabell presenteras riskerna kopplade till identifierade iakttagelser:

#	Iakttagelse	Risk	Risknivå
4.2	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 av kontrollera att alla applikationsförändringar som driftsätts följer myndighetens processer och kontroller för applikationsförändring, 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
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 produktionsmiljön.	Medel
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
4.5	Bristande spårbarhet gällande testning av applikationsförändringar	Bristande spårbarhet i applikations-förändringsprocessen gällande testning försvårar arbetet vid en eventuell felsökning. Risken ökar även för att fel oavsiktligt förs in i produktionsmiljön på grund av oaktsamhet.	Hög
4.6	Otillräckliga automatiska kontroller vid behörighetsbeställning i BOA	Att behörigheter kan beställas av personer som inte är berättigade att beställa till en given medarbetaren 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

4.7	Avsaknad av säkerhets-prövning 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**
4.8	Informella rutiner och otydlighet kring högre (privilegierade) IT-behörigheter	De informella processer för behörighets-hantering 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**
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**
4.10	Brister i periodisk genomgång av behörigheter	Att regelbundna genomgångarna 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**
4.11	Avsaknad av skriftlig överenskommelse med Försäkringskassans för hantering av höga IT-behörigheter	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**
4.12	Avsaknad kontroll av genomförd säkerhetsutbildning	Avsaknad av regelbundna informationssäkerhetsutbildningar innebär risk för att för verksamheten känslig och kritisk information behandlas på ett icke tillfredsställande sätt ur ett säkerhetsperspektiv, vilket kan resultera i att informationen kommer obehörig part till handa.	**Låg**

Identifierade iakttagelser och rekommendationer för att hantera dessa beskrivs mer ingående nedan.

4.2 Systemgenererade listor över applikationsförändringar kan för närvarande inte produceras

4.2.1 Iakttagelse

Vid vår granskning noterade vi att Försäkringskassan under 2011 har implementerat ett CMDB[20]-verktyg som kan möjliggöra utsökning av systemgenererade listor över sådant som har driftsatts inom ett visst tidsintervall. Dock finns ännu ingen funktionalitet i verktyget som gör det möjligt att söka ut en förändringslista på ett smidigt sätt.

4.2.2 Risk

Låg	Avsaknad av fullständiga listor över applikationsförändringar som har driftsatts innebär att det finns begränsade möjligheter av kontrollera att alla applikationsförändringar som driftsätts följer myndighetens processer och kontroller för applikationsförändring, 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.

4.2.3 Rekommendation

Vi rekommenderar att Pensionsmyndigheten verkar för att Försäkringskassan överväger möjligheten att implementera funktionalitet som gör det möjligt att ta ut systemgenererade listor över driftsatta applikationsförändringar i myndighetens kritiska system. Viktigt är att funktionaliteten utformas på sådant sätt att den inte går att kringgå, dvs. att samtliga driftsättningar automatiskt registreras.

4.2.4 Status

Kvarstående iakttagelse sedan tidigare granskning.

[20] Configuration management database (CMDB) är en databas med information relaterad till ett IT-systems komponenter.

4.3 Osäker ändringsrutin för standardändringar i COBOL

4.3.1 Iakttagelse

Under granskningen har vi noterat att vissa typer av applikationsförändringar inte kräver godkännande av utveckling från lokal Change Manager eller CAB-godkännande för produktionssättning. Detta gäller vad som klassats som standardändringar, däribland ändringar med COBOL-kodning, som istället omfattas av ett övergripande förhandsgodkännande. COBOL-kodningar används för vissa delar av handläggningssystemen gällande dagersättning och bidrag samt vissa delar av pension och mindre förmåner. Uppskattningsvis är 35-40% av Försäkringskassans programstock COBOL-kodad, det är dock oklart hur stor ande av Pensionsmydnighetens programkod som är COBOL-baserad. Testningen av dessa COBOL-ändringar genomförs av ändringsplanerare.

4.3.2 Risk

Medel	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 produktionsmiljön.

4.3.3 Rekommendation

Vi rekommenderar att Pensionsmyndigheten verkar för att Försäkringskassan att se över ändringsrutinerna för COBOL-ändringar, främst gällande ansvarsfördelningen kring utveckling och testning, men också utvärdera hur man säkerställer att icke avsedda eller otillräckligt testade COBOL-ändringar inte produktionssätts.

4.3.4 Status

Kvarstående iakttagelse sedan tidigare granskning.

4.4 Bristande tydlighet i hur nödvändiga testnivåer fastställs

4.4.1 Iakttagelse

Vid vår granskning noterade vi att Försäkringskassan har ett antal olika testnivåer som används för att verifiera utvecklad IT-funktionalitet. Däremot finns ingen dokumentation som specificerar nödvändiga testnivåer för olika typer av aktiviteter alternativt en rutinbeskrivning för hur nödvändiga testnivåer ska fastställas.

4.4.2 Risk

Låg	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.

4.4.3 Rekommendation

Vi rekommenderar att Pensionsmyndigheten verkar för att Försäkringskassan att dokumentera nödvändiga testnivåer för olika typer av ändringar alternativt annat stöd för beslut om nödvändiga testnivåer. Vidare bör myndigheten fastställa vilken roll som har ansvaret att ta beslut rörande testplanering.

4.4.4 Status

Kvarstående iakttagelse sedan tidigare granskning.

4.5 Bristande spårbarhet gällande testning av applikations-förändringar

4.5.1 Iakttagelse

Under granskningen har utvalda applikationsförändringar undersökts bland annat avseende att dessa hade testats och godkänts innan produktionssättning, samt att detta hade dokumenterats. För fem (5) av 30 testade förändringarna har vi dock inte kunnat ta del av någon dokumentation som visar på att testning är genomförd.

Detta föranledde en utökad testning av ytterligare 30 förändringar. För 17 av de 30 efterfrågade förändringarna har vi inte kunnat ta del av någon dokumentation som visar på att testning är genomförd.

4.5.2 Risk

Hög	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.

4.5.3 Rekommendation

Vi rekommenderar att Pensionsmyndigheten verkar för att Försäkringskassan tar fram en rutin för hur testfall och testdokumentation ska upprättas och sparas samt tillser att denna rutin följs.

4.5.4 Status

Kvarstående iakttagelse sedan tidigare granskning.

4.6 Otillräckliga automatiska kontroller vid behörighetsbeställning i BOA

4.6.1 Iakttagelse

För att vara berättigad att beställa behörigheter måste en anställd inneha behörighetsrollen *Chef*. Rollen *Chef* kan begränsas med ett behörighetsområde, vilket är detsamma som det kontor personen arbetar på, eller för vissa roller inkludera hela Försäkringskassan. Behörighetsområdet begränsas automatiskt i BOA och hindrar en chef från att kunna lägga beställningar på behörigheter till personer utanför behörighetsområdet. Enligt Försäkringskassans riktlinjer ska närmaste chef ansvara för att beställa nya behörigheter, något som inte automatiserat kontrolleras av systemet. Kontroll av närmaste chef görs istället manuellt av behörighetsadministrationen genom manuella kontroller. Vi har också uppmärksammat att BOA inte kan varna för känsliga behörighetskombinationer. Även här förlitar man sig på en manuell kontroll som utförs av Behörighetsadministrationen, vilken inte täcker samtliga förmånssystem.

4.6.2 Risk

Medel	Att behörigheter kan beställas av personer som inte är berättigade att beställa till en given medarbetaren 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.

4.6.3 Rekommendation

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.

4.6.4 Status

Kvarstående iakttagelse sedan tidigare granskning.

4.7 Avsaknad av säkerhetsprövning för personal med höga IT-behörigheter

4.7.1 Iakttagelse

Pensionsmyndigheten har i vägledande principer för samarbete[21] ställt krav på att personal vid Försäkringskassan som har arbetsuppgifter enligt vissa specificerade kriterier ska genomgå säkerhetsprövning enligt säkerhetsklass 2. Det berör bland annat områden som relaterar till höga IT-behörigheter.

Genom intervjuer vid Försäkringskassans IT så har det framkommit att detta inte sker rutinmässigt enligt formellt fastställd rutin eller process. Det är dock något som man belyst som ett behov inom Försäkringskassan under det gångna året.

4.7.2 Risk

Medel	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.

4.7.3 Rekommendation

Vi rekommenderar att Pensionsmyndigheten verkar för att Försäkringskassan säkerställer efterlevnad och uppföljning av säkerhetsprövning av roller som har identifierats ha tillgång till känslig eller stor mängd information, så att det vid var tid avspeglar gällande informationssäkerhetskrav och avtal mellan myndigheten.

4.7.4 Status

Ny iakttagelse identifierad under denna granskning.

[21] Vägledande principer för samarbetet mellan FK och PM v2.0 (2012-12-10)

4.8 Informella rutiner och otydlighet kring högre (privilegierade) IT-behörigheter

4.8.1 Iakttagelse

IT pekas ut som ansvarig för hantering av IT-behörigheter i Försäkringskassans informationssäkerhetsriktlinje[22] för behörighetsadministration. I riktlinjen finns dock inte specificerat vilken typ av behörighet som klassas som IT-behörighet. Hittills har IT-avdelningen gjort en tolkning av vilka behörigheter som ska klassas som IT-behörigheter.

Inom Försäkringskassan finns ett regelverk gällande beställning av nya behörigheter där det framgår att ansvarig chef ska vara beställare av behörigheter. För privilegierade IT-behörigheter följs inte detta regelverk utan enskilda teknikområden har istället egna informella processer för nyupplägg. Det innebär också att dokumentationen kring upplagda behörigheter är bristfällig. Som ett led i detta saknas också rutiner för borttag av gamla behörigheter samt periodiska genomgångar. IT-säkerhetschef gör sporadiska genomgångar när antalet personer med behörigheter upplevs som stort.

Då IT-avdelningen och Säkerhetsstaben har identifierat dessa problem med informella processer och begränsad spårbarhet har inlett ett projekt för implementering av ett IAM-system för hantering av behörigheter under 2013 enligt föreslagen utvecklingsplan. Projektet och IAM-systemet ska vara infört under 2014. 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.

4.8.2 Risk

Medel	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.

4.8.3 Rekommendation

Ett arbete pågår vid Försäkringskassan med att implementera ett IAM-system för ökad kontroll av behörighetshanteringen, vilket ska vara infört under 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 man går vidare med detta arbete, samt att man utreder, identifierar och specificerar vilka behörigheter som ska hanteras av IT respektive Behörighetsadministration.

[22] Riktlinjer för informationssäkerhet - behörighetsadministration v1.2, 2010:5.

4.8.4 Status

Kvarstående iakttagelse sedan tidigare granskning.

4.9 Mindre brister i hantering av SID-behörigheter

4.9.1 Iakttagelse

Vid upplägg av en ny SID-behörighet görs idag en manuell kontroll av att den som har lagt beställningen av behörigheten är en så kallad SID-chef alternativt säkerhetschef på myndigheten. Försäkringskassan har infört en kompenserande detektiv kontroll där myndigheten månatligen går igenom tilldelade SID-behörigheter och återrapporterar dessa till Pensionsmyndigheten.

4.9.2 Risk

Låg	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.

4.9.3 Rekommendation

Vi rekommenderar att man undersöker möjligheterna att i BOA lägga in en automatisk kontroll av beställande chef vid beställning av SID-behörigheter där enbart SID-chefer ska kunna beställa behörigheten. Då felaktig SID-behörighet eller beställning kan ge avsevärda konsekvenser för enskild person rekommenderar vi Försäkringskassan att hantera felaktig och obehörig beställning av SID-behörighet som en säkerhetsincident.

4.9.4 Status

Kvarstående iakttagelse sedan tidigare granskning.

4.10 Brister i periodisk genomgång av behörigheter

4.10.1 Iakttagelse

För att säkerställa att obehöriga inte har tillgång till system som används av Pensionsmyndigheten eller anställda innehar felaktiga behörigheter måste användarbehörigheter tas bort vid avslutad anställning eller vid byte av arbetsuppgifter inom Pensionsmyndigheten. En kompenserande kontroll har därför införts där Försäkringskassans Behörighetsadministration tar del av lönelistor för Pensionsmyndigheten via Statens Service Center, vilka sedan jämförs med aktuella behörigheter och där man avslutar de som inte finns representerade på lönelistan.

Vid intervjuer med Behörighetsadministrationen framkom det att det brustit i den månadsvisa kontrollen då lönelistor inte gjorts tillgängliga för Behörighets-administrationen sedan sommaren 2013. Detta var vid granskningens tillfälle noterat av både Pensionsmyndigheten och Försäkringskassan, men man hade inte fortsatt arbetet med att identifierat bristen för att möjliggöra en lösning på problemet.

4.10.2 Risk

Låg	Att regelbundna genomgångarna 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 Pensionsmyndigheten fortsatt innehar känsliga behörighetskombinationer.

4.10.3 Rekommendation

Vi rekommenderar Pensionsmyndigheten att titta över anledningen till varför rutinerna brustit och åtgärda problemen för att minimera risken för att det inträffar igen.

4.10.4 Status

Ny iakttagelse identifierad under denna granskning.

4.11 Avsaknad av skriftlig överenskommelse med Försäkringskassans för hantering av höga IT-behörigheter

4.11.1 Iakttagelse

Under granskningen av Pensionsmyndigheten har det framkommit under intervjuer att dokumenterade tjänsteöverenskommelser rörande behörighetshantering av höga IT-behörigheter saknas. Det vill säga avtal mellan Pensionsmyndigheten och Försäkringskassan med specifika krav avseende exempelvis nyckelkontroller, mätetal och rapportering. Ett övergripande avtal finns mellan myndigheterna, men det finns inga specifika krav i ett så kallat SLA för tjänsten och de system som omfattas.

4.11.2 Risk

Medel	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.

4.11.3 Rekommendation

Vi rekommenderar Pensionsmyndigheten att säkerställa att tjänsteöverenskommelser arbetas fram och avtalas för tjänster och system som handhas av externa parter, i detta fall Försäkringskassan och hantering av höga IT-behörigheter.

4.11.4 Status

Ny iakttagelse identifierad under denna granskning.

4.12 Avsaknad kontroll av genomförd säkerhetsutbildning

4.12.1 Iakttagelse

Pensionsmyndigheten har i riktlinjer[23] ställt krav på att samtliga medarbetare ska ha genomfört en grundläggande säkerhetsutbildning för ett erhålla grundläggande åtkomst i system (PM Bas). Vidare har de ställt krav på att innan åtkomst ges till verksamhetssystem som utgör en del av socialförsäkringens administration, ska en fördjupad verksamhets-utbildning vid behov ha genomgåtts.

Pensionsmyndigheten genomför regelbunden utbildning av sin personal i informationssäkerhet, bland annat med hjälp av DISA[24] samt även med förmedlad utbildning. Initialt genomförde Pensionsmyndigheten en omfattande utbildningsinsats där man även dokumenterade vilka som genomfört utbildningen, men det är inget som myndigheten fortlöpande fortsatt med och det sker ingen dokumenterad kontroll vid tilldelning av behörigheter.

4.12.2 Risk

Låg	Avsaknad av regelbundna informationssäkerhetsutbildningar innebär risk för att för verksamheten känslig och kritisk information behandlas på ett icke tillfredsställande sätt ur ett säkerhetsperspektiv, vilket kan resultera i att informationen kommer obehörig part till handa.

4.12.3 Rekommendation

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.

4.12.4 Status

Ny iakttagelse identifierad under denna granskning.

[23] Riktlinje säkerhet för chefer v2.0

[24] Datorstödd informationssäkerhetsutbildning för användare (DISA) som ges ut av Myndigheten för samhällsskydd och beredskap.

Bilaga 1: Metod

Uppdraget har utförts genom intervjuer med nyckelpersonal, identifiering av nyckelkontroller och genom granskning av relevant dokumentation och information i system. Identifiering av nyckelpersoner och nyckelkontroller har skett i samarbete med företrädare från Pensionsmyndigheten.

Granskningen har omfattat följande steg

- Planering med ansvariga från Riksrevisionen
  - Riksrevisionen och Transcendent Group fastställde omfattningen av granskningen
  - Riksrevisionen informerade intressenter om avsikten att genomföra revision
  - Granskningsprogram fastställdes
- Uppstartsmöte med företrädare från Pensionsmyndigheten
  - Övergripande beskrivning av genomförande
  - Övergripande identifiering av nyckelpersoner för informationsinsamling
  - Förberedande arbete inför granskning
- På-plats-granskning
  - Intervjuer
  - Visuella granskningar
  - Stickprov
- Analys
  - Riskbedömning
  - Konsekvensbedömning
  - Faktaavstämning
- Rapportering
  - Skriftlig i utkast
  - Färdig rapport

Planering

Upprättande av uppdragsbeskrivning som godkänts av ansvarig revisor på Riksrevisionen innan arbetet påbörjats.

Informationsinsamling/utvärdering

- Inläsning av material i form av styrande dokument som riktlinjer för säkerhet och processbeskrivningar

- Intervjuer med ansvariga för behörighetshantering och systemförändringar i syfte att få processer och nyckelkontroller beskrivna, samt vilka åtgärder som vidtagits avseende tidigare iakttagelser
- Insamling av kompletterande dokumentation efter informationsinsamling och intervjuer
- Inläsning och granskning av kompletterande material
- Sammanställning och analys samt kompletterande intervjuer.

Följande personer har intervjuats inom ramen för granskningen:

Namn	Roll
Anders Tillgren	Säkerhetsspecialist
Daniel O Andersson	Enhetschef för Utveckling och Test
Ing-Britt Holmqvist	Förvaltningsledare pensionsprodukter samt tjänsteansvarig för IT-tjänster som köps av FK.
Josefin Östfeldt	IT-säkerhetsansvarig och enhetschef för IT-säkerhet, projektägare till projektet höga behörigheter.
Karl Solnestam	Säkerhetsspecialist (Konsult).
Lena Mahlberg	Chef Drift och infrastrukturenheten
Peter Westberg	Säkerhetsspecialist (Konsult).
Joakim Lundberg	Verksamhetsspecialist, Försäkringskassans behörighetsadministration
Örjan Lindgren	Verksamhetsspecialist, Försäkringskassans behörighetsadministration
Eva Rehnberg	Verksamhetsspecialist, Försäkringskassans behörighetsadministration

Följande dokument har använts som stöd för granskningens resultat:

Dokument	Version
234_Beställning_Behörighetsadministration_adminbehörigheter.doc	2011-10-20
BA ansvar o servicenivå matris 1.2_rev1.doc	1.2_rev1
BA Tjänstebeskrivning 1.3_rev1.doc	1.3_rev1
Handlingsplan nyckelkontroller generella behörigheter.pdf	v1.1
Kontrollbeskrivning Teknik- och systemadministrativa behörigheter v1 0.docx	v1.0
Nyckelkontroller_Behörighetsprocessen_Användarbehörigheter.pdf	v1.1
PID100318_v2.0+Riktlinje+säkerhet+för+medarbetare.pdf	v2.0
PID100319_v2.0+Riktlinje+säkerhet+för+chefer.pdf	v2.0
PID100320_v2.0+Riktlinjer+för+säker+IT.pdf	v2.0
PID101483_v2 0 Särskild instruktion behörighetstilldelning FK_PM.pdf	v2.0
PID103938_v1.3 Utvärdering av tilldelade behörigheter.doc	v1.3
PID120361_v1.1 Nyckelkontroller Behörighetsprocessen.docx	v1.1
PID124022_v2.0 Pensionsmyndighetens rutiner för eTjänstekort.docx	v2.0
PID126985_v1.0+Strategidokument+IAM.pdf	v1.0
PID130005_v2.0+Vägledande+principer+för+samarbetet+mellan+FK+och+PM[1].pdf	v2.0
PM-rapport BA 2013 v2.xlsm	v2
Rutin för utvärdering av tilldelade behörigheter	v1.3
PID112291_v3.1_Handledning_Projekt_på_Pensionsmyndigheten	v3.1
BUL- Processen projekt	v1.3

Applikationer som urval slumpats ifrån

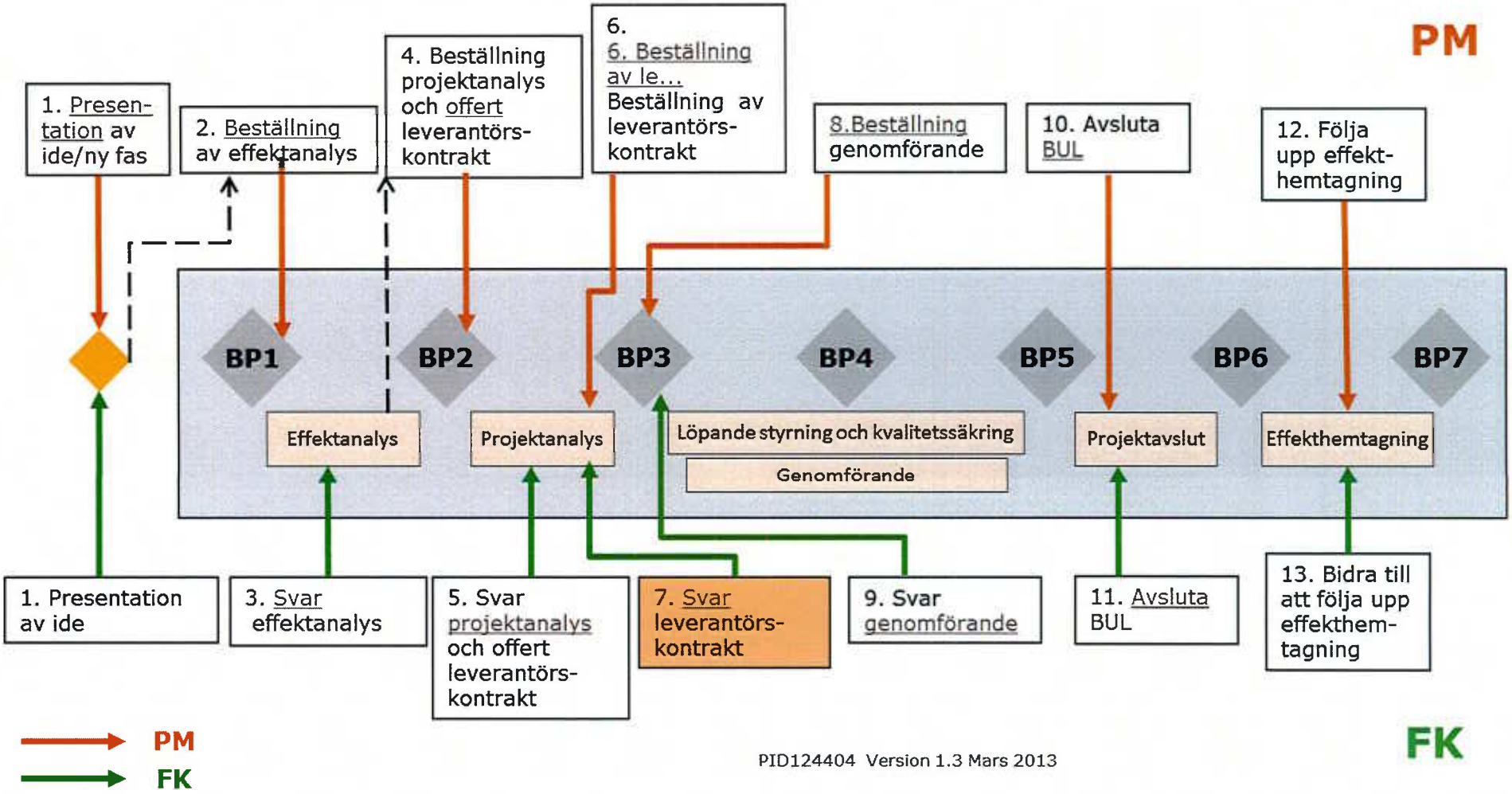
Vid de kontrolltester som utförts inom ramen för detta arbete har stickprov tagits från följande applikationer. Värt att notera är att urvalet gjorts slumpmässigt vilket innebär att alla applikationer inte behöver finnas representerade i testresultatet. Däremot ska de testade kontrollerna tillämpas oberoende av applikation, vilket innebär att testningen utgör ett underlag även för applikationer som inte finns med i urvalet.

Applikation
Ålderspension 37
Ålderspension 38
Efterlevandepension
Bostadstillägg till pensionärer
Särskilt pensionstillägg

Rapportering

- Upprättande av preliminär rapport med beskrivning av granskade områden, iakttagelser och förslag på förbättringsåtgärder
- Verifiering av iakttagelser och förbättringsförslag med nyckelpersoner
- Presentation av slutrapport till Riksrevisionen.

Bilaga 2: BUL-processen för projekt



PID124404 Version 1.3 Mars 2013