transcendent group GOVERNANCE RISK COMPLIANCE

IT-revision vid Försäkringskassan

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 Försäkringskassan anlitat Transcendent Group för att utföra en granskning av generella IT-kontroller avseende hantering av behörigheter och systemförändringar kopplat till förmåns- och utbetalningssystemen vid Försäkringskassan.

Syftet med granskningen har varit att bedöma huruvida hantering av behörigheter och systemförändringar avseende Försäkringskassans applikationer (och därtill hörande databaser och operativsystem) inom processer för anslagsfinansierade förmåner 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

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.

Försäkringskassan 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.

Försäkringskassan rekommenderas även att utöka BOA:s funktionalitet till att inkludera spärrar som gör att endast berättigad chef kan beställa behörigheter samt utreda vilka behörighetskombinationer i förmånssystemens roller och profiler som ej är tillåtna. Vidare rekommenderas Försäkringskassan att säkerställa efterlevnad och uppföljning av säkerhetsprövning för roller som har identifierats ha tillgång till känslig eller stor mängd information, samt tillse att periodiska behörighetsgenomgångar för priviligierade behörigheter inom IT regelbundet genomförs.

2014-01-20

Andreas Ericson

Uppdragsledare

Joachim Klasson

IT-revisor

Innehåll

1. Inledning

1.1. Uppdrag

Transcendent Group har på uppdrag av Riksrevisionen utfört en granskning av generella IT-kontroller avseende hantering av behörigheter och systemförändringar kopplat till förmåns- och utbetalningssystemen vid Försäkringskassan. Uppdraget är ett avrop av Riksrevisionens av ingånget ramavtal (diarienummer Riksrevisionen 38-2011-1507).

1.2. Syfte och omfattning

Syftet med revisionen har varit att bedöma huruvida hantering av behörigheter och systemförändringar avseende Försäkringskassans applikationer (och därtill hörande databaser och operativsystem) inom 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
- Test av ett lämpligt urval av ovan identifierade IT-generella kontroller

1.3. Avgränsningar

Målet med denna granskning har varit att säkerställa kvalitet i IT-organisationens processer för hantering av systemförändringar och hantering av behörigheter. Inom ramen för denna granskning har Transcendent Group således inte beaktat hur Försäkringskassans och Pensionsmyndighetens verksamheter bidragit till styrning av projekt i myndigheternas utvecklingsplaner.

Vår granskning inom dessa två områden har baserats på intervjuer och stickprov[1]. Denna omfattning är i sig inte tillräcklig för att identifiera samtliga brister som kan förekomma i myndighetens processer. Granskningens omfattning syftar därför till att vi med rimlig säkerhet ska kunna identifiera de mest kritiska riskerna.

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

1.3.1. 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

[1] 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.

kontroller som bedömts vara mest signifikanta för att minska risken för felaktiga applikationsförändringar i Försäkringskassans IT-system.

Urvalet av applikationsförändringar som ovanstående kontroller har testats mot kommer från applikationer där felaktiga förändringar skulle kunna leda till att ersättningar blir felaktiga eller att utbetalning inte går att genomföra. Dessa applikationer[2] identifierades vid 2011 års granskning i samråd med Riksrevisionen, dåvarande revisionsstöd och Försäkringskassan. Riskrevisionen har i denna granskning beslutat att behålla samma omfattning och urval av applikationer.

1.3.2. Behörighetshantering

Även behörighetshantering kan innefatta ett stort antal kontroller. Vi har under denna testning fokuserat på förändringar av behörigheter samt periodiska genomgångar av behörigheter i utvalda 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] Se bilaga 1 för en översikt över de system som granskats.

2. Försäkringskassans IT-organisation

Försäkringskassans IT-organisation är en av Sveriges största med cirka 870 anställda, runt 200 konsulter och en kostnad på ungefär 1,5 mdkr. Försäkringskassan satsar cirka 680 miljoner kronor under 2012 och 700 miljoner kronor under 2013 på verksamhetsutveckling med IT-inslag där en stor del är i syfte att öka kundservicen och höja produktiviteten.

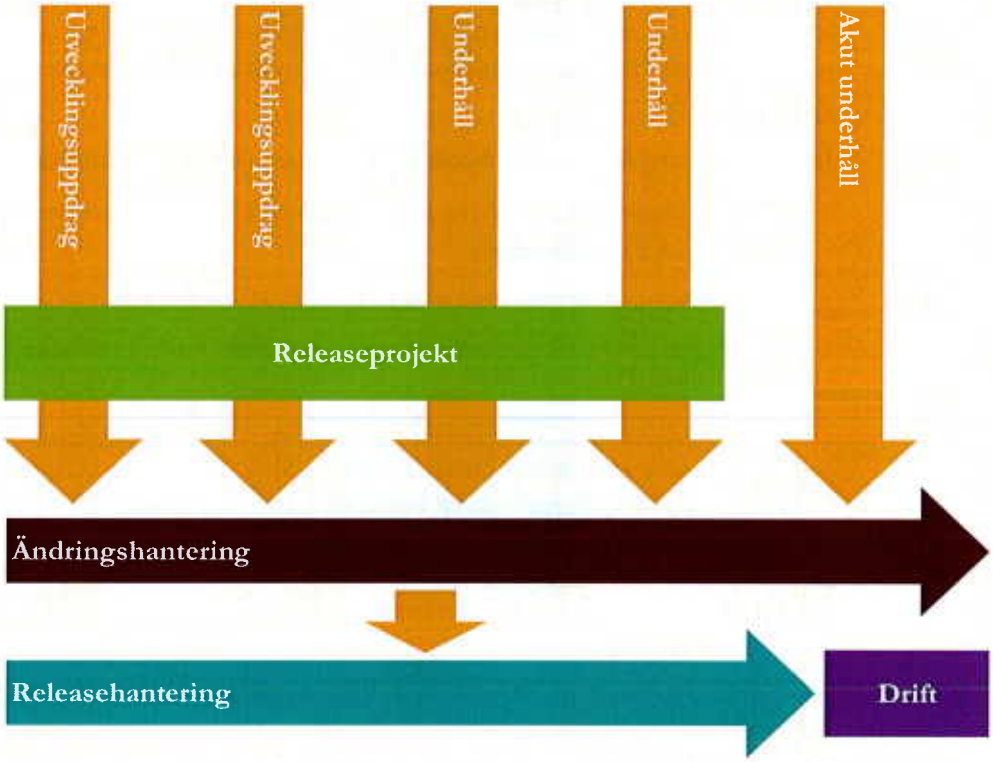
Inom Försäkringskassans IT-organisation finns tre verksamhetsområden (VO):

- VO Applikation (ITA) deltar i utvecklingsprojekt fram till överlämnande till VO Produktion för driftsättning.
- VO Produktion (ITP) driftar Försäkringskassans och några av Pensionsmyndighetens IT-system och ansvarar för att driftsätta de applikationsförändringar som VO Applikation (ITA) utvecklat.
- VO Tjänsteleverans (ITT) hanterar Försäkringskassans beställarrelationer (interna och externa), avtal och överenskommelser, SLA (Service Level Agreement), förvaltningsstyrning, samt ger stöd till Försäkringskassans verksamhet och till externa partners i IT-frågor. Kopplat till denna granskning koordinerar de även kontakten med Försäkringskassans och Pensionsmyndighetens verksamheter och bevakar deras behov.

Inom ITA och ITP finns ett antal stödenheter, se bilaga 4 för en mer komplett organisationskarta tillhandahållen av Försäkringskassan.

Att IT-organisationen är stor ställer krav på ett strukturerat arbetssätt med formella processer och verktygsstöd. Vår uppfattning är att omfattningen av processdokumentation är stor, vilket kan göra det svårt att använda sig av denna dokumentation för att snabbt skapa sig en överskådlig förståelse för hela processen.

3. Granskning av processer för systemförändring



Aktiviteter som syftar till att förändra applikationer i Försäkringskassans IT-miljö kan delas in i två övergripande kategorier:

- Utvecklingsprojekt registreras alltid i Uppdragsdatabasen och kan utgöras av:
  - Projekt i Försäkringskassans eller Pensionsmyndighetens utvecklingsplan
  - Departementsuppdrag
  - Mindre vidareutveckling (under en viss beloppsgräns)
- Underhållsprojekt utgörs av mindre buggfixar som oftast initieras i incident- och problemhanteringsprocesserna.

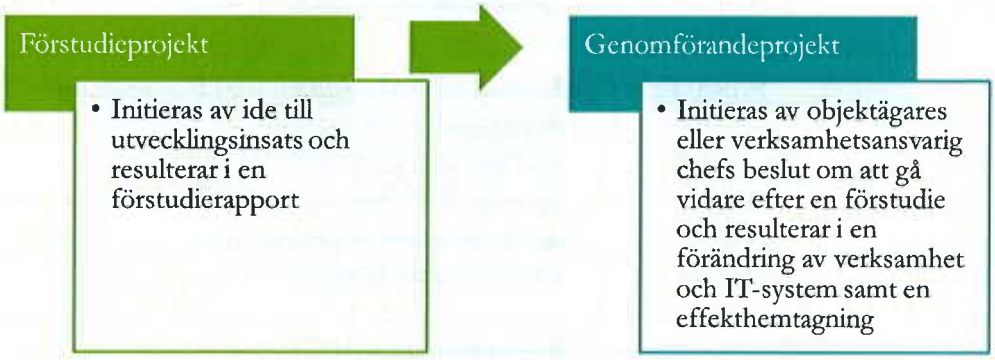
Dessa kategorier hanteras i två skilda processer, med vissa gemensamma steg såsom utförande av tester, men koordineras oftast i ett så kallat releaseprojekt[3].

Driftsättning sker efter att ärendet har passerat processerna för ändrings- och releasehantering[4]. Kommande avsnitt innehåller en översiktlig beskrivning av dessa flöden samt viktiga beslutspunkter.

[3] Undantaget är då ett underhållsärende måste driftsättas akut.
[4] Observera att releaseprojekt inte är samma sak som releasehantering. Det förra handlar om koordinering av de kandidater som ska driftsättas vid ett releasetillfälle medan det senare är processen för driftsättning av enskilda kandidater.

3.1. Utvecklingsprojekt

Formellt är utveckling av Försäkringskassans verksamhet inklusive IT-system uppdelat i två efter varandra följande uppdrag:



Förstudiens syfte är att analysera förändringsbehovet och lämna lösningsförslag inklusive kostnads- och nyttobedömningar så att verksamhetsansvarig/ledning kan fatta beslut om fortsatt utvecklingsarbete. Under en viss beloppsgräns är förstudier inte tvingande och kan då i överenskommelse mellan verksamheten och *VO Applikation* utelämnas och i relevant omfattning bedrivas integrerat med genomförandeuppdraget. Även om dessa två projekttyper har skilda utgångspunkter och mål följer de båda samma uppdragslivscykel[5] med förbestämda steg och beslutspunkter som loggas och dokumenteras i *Uppdrags-databasen*.

Ett uppdrag inleds med tre planeringsfaser[6]:

- **FAS 1: Från behov till grovt förslag och estimat**
  I denna fas prioriterar verksamhetsansvarig en konkret idé om utveckling och IT genomför en prospektanalys genom att ta fram övergripande uppdragsplaner avseende utförande, ekonomiska implikationer och leveransdatum.
- **FAS 2: Från grovt förslag och estimat till uppdaterad utvecklingsplan**
  I början av denna fas beslutar verksamheten om uppdraget ska fortgå eller avbrytas. Efter detta förs uppdraget in i IT-planen vilket innebär att det blir en releasekandidat

[5] Denna granskning fokuserar på applikationsförändringar men det kan påpekas att samma livscykel även beskriver förändring av hårdvara, mellanprogramvara och tredjepartsprodukter.
[6] Omfattningen av det arbete som utförs i de olika faserna står i proportion till uppdragets storlek. Försäkringskassans egna processkartor för dessa planeringsfaser finns i bilaga 2.

som ska beläggas och koordineras med andra uppdrag. Uppdrag som inte räknas som mindre vidareutveckling har sin grund i Försäkringskassans eller Pensionsmyndighetens verksamhetsplan. Dessa uppdrag för ekonomistaben in i ett förslag till en reviderad utvecklingsplan baserad på input från verksamheten och IT. Efter godkännande från generaldirektören (GD) uppdateras utvecklingsplanen[7] enligt förslag.

- **FAS 3: Från uppdaterad utvecklingsplan till IT-beredning**
  I denna fas gör verksamheten en effektanalys och IT tar fram ett detaljerat förslag avseende systemutveckling som sammanställs i ett VBU (verksamhetens beslutsunderlag) som skickas till ekonomistaben. Efter en ekonomistabsberedning och en IT-beredning, där ett forum (uppdragsledning) avgör om uppdraget kan åtas, beslutar ekonomistaben om start, budget och finansiering.

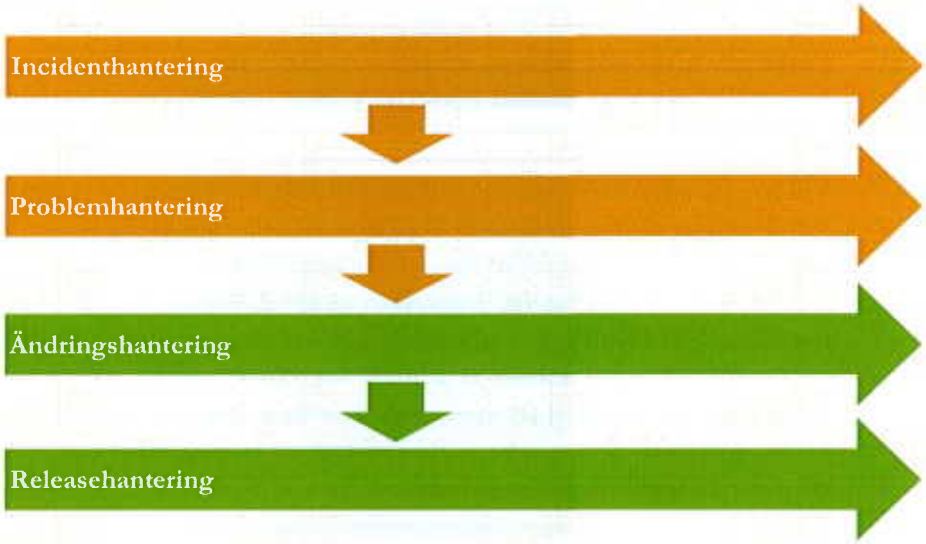
Efter ekonomistabens beslut om att projektet ska startas påbörjar *VO Applikation* utvecklingsarbetet enligt plan. Efter att detta har slutförts utför projektet tester[8] (se avsnitt 3.3) av den utvecklade funktionaliteten varefter projektets styrgrupp beslutar att utvecklingsprojektet ska ingå i en release (se avsnitt 3.4).

Efter produktionssättning avslutas projektet efter ett enat beslut från verksamheten och IT. Uppföljning av projektets effekter görs inom verksamheten en tid efter avslutat projekt.

3.2. Underhållsprojekt

Försäkringskassan har en ITIL[9]-baserad process för underhåll av IT-system. Detta innebär att en ändring kan ha sitt ursprung i ett problemärende, som i sin tur har föregåtts av en eller flera incidenter[10].

[7] Utvecklingsplanen innehåller förutom pågående projekt även uppdrag i Fas 2 och Fas 3. IT arbetar kontinuerligt med att planera och koordinera de aktiviteter som finns i utvecklingsplanen. *VO Applikation* ser en viss problematik i verksamhetens önskemål att även ta med uppdrag i Fas 1 i utvecklingsplanen. Detta skulle resultera i en starkt föränderlig utvecklingsplan som skulle resultera i ett ohanterligt planeringsarbete. *VO Produktion* ser dock problem i att leveransområdena alldeles för sent inför sina förändringsbehov i IT-planen vilket ökar andelen akuta ändringar.
[8] De projektdeltagare som testar applikationsförändringar arbetar inom testenheten.
[9] ITIL, akronym för 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.
[10] Se Försäkringskassans mer detaljerade processkartor i bilaga 3.



Efter att bedömningen har gjorts att det krävs en applikationsförändring för att ett identifierat problem ska lösas skrivs en ändringsbegäran och ärendet går in i processen för ändrings- och releasehantering (se avsnitt 3.5). Ett underhållsärende koordineras i normalfallet inom ramen för en release, men kan baserat på beslut från CAB[11] driftsättas akut, det vill säga utanför en release. I båda fallen följer dock ärendet processerna för ändrings- och releasehantering.

3.3. Utförande av tester

Försäkringskassan arbetar med ett antal nivåer för testning av applikationsförändringar som används oavsett om förändringen drivs som ett utvecklingsprojekt eller underhållsprojekt:

- **Enhetstest** verifierar en enskild komponent.
- **Integrationstest** verifierar de komponenter som bildar avsedd funktionalitet tillsammans.
- **Systemtestnivå 1** verifierar förändringens funktionalitet samt samverkande produkter för att säkerställa att flödet fungerar.
- **Acceptanstest** verifierar att förändringen uppfyller användarbehoven. Denna nivå utförs av beställare eller verksamhetsansvarig och kan påbörjas parallellt med systemtestnivå 1.
- **Systemtestnivå 2** verifierar att hela den flödeskedja där funktionen ingår fungerar. Denna testnivå utförs för hela releaser.
- **PSV-test**[12] verifierar att releasen[13] fungerar avseende de mest verksamhetskritiska tjänsterna oavsett om de ändrats eller inte.

[11] Change Manager är behörig att fatta beslut om akut driftsättning vid icke-komplexa fall. Beslutet ska dock formaliseras vid efterkommande CAB-möte.
[12] PSV - Produktionsklar systemversion.
[13] Denna testnivå utförs endast inom ramen för releaseprojekt (se avsnitt 3.4).

För att en applikationsförändring ska gå vidare till nästa testnivå krävs att resultatet i föregående nivå dokumenteras, utvärderas och därefter godkänns av specificerad ansvarig beroende på testnivå. Samtliga testnivåer är dock inte relevanta för samtliga ändringsärenden.

Vid granskningen har vi noterat att Försäkringskassan saknar dokumenterade riktlinjer som beskriver när en viss testnivå är obligatorisk eller hur beslut tas om relevanta testnivåer. En anledning till att sådan dokumentation inte har tagits fram är att testledare vid Försäkringskassan har fått synpunkter på att riktlinjerna har varit för tunglästa och inte tillräckligt generella. Vid utbildningstillfällen för testare och testledare diskuteras dock vilka tester och testnivåer som är lämpliga vid olika förändringsaktiviteter. Enligt riktlinjer för testning[14] framgår det att testning skall planeras och genomföras enligt riskbaserad metod. Miniminivån man arbetar efter är dock att testning alltid ska finnas definierat för alla typer av applikationsförändringar.

3.4. Releaseprojekt

Processerna för utveckling och underhåll av IT-system drivs ofta som relativt autonoma projekt/uppdrag men förs samman till en hanterlig mängd och koordineras i så kallade releaseprojekt. En normal releasekalender innefattar fyra fastställda releaseprojekt per år i februari, maj, september och november. Utöver dessa kan releaseprojekt tillkomma t.ex. till följd av lagändringar.

För att göra denna koordinering praktiskt möjlig pågår löpande uppdrags- och releaseplanering med prospekt och pågående aktiviteter på olika nivåer både inom *VO Produktion, VO Applikation* samt samordnat tillsammans med ledningen för verksamhetsområden.

Vid start av projekt är det fastställt vilken/vilka releaser projektet ska leverera inom. Ungefär fem månader innan driftsättning av release, fryses releasen innehållsmässigt. Strikt ändringhantering sker sedan av releaseinnehållet. Om en deltagare i releasen vid test visar på brist som klassas som driftshindrande och som inte går att rätta till innan driftsättning, kan det uppdraget/projektet tas ur releasen. Detta är ett beslut som tas av uppdragets/projektets beställare, ibland på rekommendation av releaseprojektets styrgrupp.

Projektutförandet innefattar primärt planering, verifiering, paketering, överlämnande till produktion samt förvaltningsläggning. Överlämning till produktion innebär att de kandidater som ingår i releaseprojektet förs in i processerna för ändrings- och releasehantering (se avsnitt 3.5).

[14] Test på Försäkringskassan FK RUP, Rev E, 2009-10-01.

3.5. Ändrings- och releasehantering

Innan driftsättning skriver *VO Produktion* en ändringsbegäran[15] som ska godkännas[16] av en lokal Change Manager (LCM[17]). Även om ett releaseprojekt koordinerats ur ett lanserings- och verifieringsperspektiv hamnar det inte inom samma ändringsbegäran, utan en ändringsbegäran måste skrivas för varje kandidat som ingår i releaseprojektet.

Om kandidaten ingår i ett utvecklingsprojekt har applikationskoden oftast redan utvecklats inom ramen för projektet. För underhållsärenden inleder *VO Applikation* utvecklingsaktiviteter och ska samtidigt informera berörd ändringsplanerare om påbörjad aktivitet så att Request For Change (RFC) kan skrivas. Då koden färdigställts, testats och verifierats paketeras och överlämnas den till *VO Produktion* som stämmer av leveranssedeln mot en ändringsbegäran. Efter detta kvalitetssäkrar en QA-ansvarig de förberedelser, tester och verifieringar som utförts inom *VO Produktion* alternativt inom ramen för ett releaseprojekt. Den slutliga driftsättningen av applikationsändringen sker efter godkännande[18] från Change Advisory Board (CAB).

3.6. Test av kontroller i applikationsförändringsprocesserna

Inom ramen för denna granskning har vi identifierat ett antal kontroller som vi bedömer vara särskilt viktiga för att inte felaktiga applikationsförändringar ska kunna införas i Försäkringskassans IT-miljö. För att avgöra hur effektiva dessa kontroller är har vi utfört kontrolltester genom att utgå från ett urval av applikationsförändringar som under året har förts in i Försäkringskassans driftmiljö och därefter avgöra om dessa har passerat identifierade kontrollpunkter[19]. Om det skulle visa sig att en kontroll inte har gjorts är det en indikation på att kontrollen kan kringgås i samband med applikationsförändring vilket ökar risken för att felaktiga applikationsförändringar flyttas till myndighetens produktionsmiljö.

Den genomförda testningen är övergripande för alla förmånssystem, inklusive de som används av Pensionsmyndigheten. Detta eftersom alla system innefattas av samma applikationsförändringsprocess.

Den population av applikationsförändringar som använts inom våra tester är inte systemgenererad vilket i allmänhet är det önskvärda men ofta inte är möjligt. Samtliga förändringar som ska produktionssättas läggs upp i systemet Klistret, vilket skulle vara ett

---

[15] Även kallad Request for Change (RFC). Den dokumenteras i systemet BMC Remedy ARS som används av Försäkringskassan för stöd och spårbarhet i ITIL-processerna.

[16] Undantaget är de ändringskategorier som CAB klassat som standardförändringar (dessa kan aldrig vara högriskändringar) samt daglig drift eller löpande underhåll med minimal risk för oönskad påverkan.

[17] Lokal Change Manager ansvarar för den operativa ändringshanteringen inom ett leveransområde på *VO Produktion*.

[18] Samtliga CAB-möten protokollförs.

[19] Viktigt att notera är att det är Försäkringskassans processer för applikationsförändring som har testats och inte enskilda applikationer. Detta innebär att resultatet ger indikationer på graden av kontroll för samtliga applikationer som hanteras enligt testade processer. Enligt myndigheten hanteras samtliga applikationer som legat till grund för testpopulationen (se bilaga 1) enligt samma process. Inget i våra tester tyder på att någon applikation skulle avvika från processen.

alternativ för att plocka ut förändringar. Den skulle ge en mer produktionsnära källa, men inte vara mer tillförlitlig då den inte visar faktiska förändringar i produktionsmiljön. Populationen har hämtats från verktyget ARS som används av *VO Produktion* för stöd och spårbarhet i ITIL-processerna.

De risker som uppstår, avseende fullständighet, då testpopulationen inte kan baseras på systemgenererade listor från målsystemen minskas på grund av följande orsaker:

- VO Produktion driftsätter utifrån leveranssedlar från VO Applikation som kontrolleras mot ändringsbegäran i verktyget ARS.
- VO Produktion har inte tillgång till källkod för Försäkringskassans applikationer.
- VO Applikation har inte systembehörighet att driftsätta förändringar.

3.6.1. Testade kontroller

Vid våra tester har vi för var och en av förändringarna i vårt stickprov följt upp följande kontrollaktiviteter och förhållanden i relevant omfattning:

- Godkännande av ändringsbegäran från lokal Change Manager
- Godkännande av utförda testaktiviteter
- Matchning av leveranssedel mot ändringsbegäran
- Godkännande för driftsättning från CAB
- Ansvarsfördelning mellan utveckling och drift

3.6.2. Urval av applikationsförändringar

Inom denna granskning har urvalet av applikationsförändringar som ovanstående kontroller testats mot kommit från de applikationer där felaktiga förändringar skulle kunna leda till att ersättningar blir felaktiga eller att utbetalning inte går att genomföra[20].

Försäkringskassan har tre huvudsakliga handläggningsytor – *ÄHS, Din Arbetsplats* och *TP Sundsvall*. Via dessa handläggningsytor kommer handläggare åt förmånssystemen där rätten till ersättning utreds och därefter beviljas eller avslås. I de fall ersättning beviljas skickas ett beslut om utbetalning till *Utbetalningssystemet*. Tandvårdsstödet har en egen handläggningsyta eftersom handläggningen till stor del utförs automatiskt. Detta innebär också att utbetalningen av ersättning genomgår en separat process vilken är kopplad till IT-applikationen Tandvårdsstödet.

De applikationer som primärt anses vara signifikanta för Försäkringskassans och Pensionsmyndighetens utbetalningar är *Utbetalningssystemet* och de förmånssystem där ersättning beviljas[21]. Således har urvalet av de applikationsförändringar som använts för att testa myndighetens kontroller tagits från dessa applikationer. Handläggningsytorna

[20] För mer information angående granskningens avgränsning se avsnitt 1.3.1.

[21] Se bilaga 1 för en fullständig förteckning över applikationer som urvalet av applikations förändringar har tagits från. Värt att notera är att urvalet gjorts slumpmässigt vilket innebär att alla applikationer inte behöver finnas representerade. Däremot ska de testade kontrollerna tillämpas oberoende av applikation, vilket innebär att testningen ger implikationer även på applikationer som inte finns med i urvalet.

ÄHS, *DinArbetsplats* och *TP Sundsvall* är dock inte lika kritiska eftersom felaktiga förändringar inom någon av dessa applikationer enbart kan innebära påverkan på nivån av åtkomst till förmånssystemen. Detta skulle sannolikt inte leda till felaktiga ersättningar utan snarare att Försäkringskassan inte kan leva upp till sina åtagna handläggningstider.

Vid våra kontrolltester användes verktyget ARS till att generera en lista över de förändringar som gjorts under 2013[22] i samtliga förmånssystem nämnda i bilaga 1. Den fullständiga listan, som bestod av totalt 531 applikationsförändringar, inkluderade även förändringar som ännu inte var fullkomligt genomförda. Antalet slutförda förändringar inom ramen för testningen var 392 stycken varav 30 applikationsförändringar[23] slumpmässigt valdes ut för närmare granskning.

3.6.3. Resultat

Vi har vid våra tester identifierat ett antal brister, vilka vi bedömer i olika grad kan påverka respektive applikationskontrolls funktion (se även avsnitt 5). Utöver det har testerna givit oss en djupare förståelse för myndighetens processer och därmed gjort det möjligt för oss att identifiera några områden där processerna skulle kunna förbättras eller tydliggöras (se avsnitt 5).

Kontroll	Genomförd testning	Resultat
Godkännande av ändrings-begäran från lokal Change Manager	Under testningen säkerställde vi att samtliga applikations-förändringar hade inletts med ett godkännande från lokal Change Manager vilket sker genom att Change Manager flyttar ärendet från "Request for Change" till "Planning in Progress" i BMC Remedy User24. Detta är en förutsättning för att kunna gå vidare i förändringshanteringen. För vissa typer av förändringar, s.k. standardändringar, har detta steg i processen konfigurerats bort för att effektivisera processen. Dessa är återkommande ändringar som genom övergripande beslut är förgodkända och därför kan förbigå denna kontroll.	Samtliga ändringar som är berörda av kontrollen har godkänts.

[22] 2013-01-01 till 2013-10-23.
[23] I enlighet med Riksrevisionens testmetodik
[24] Används för alla ITIL-processer. Även kallad Request for Change (RFC). Den dokumenteras i systemet BMC Remedy ARS som används av Försäkringskassan för stöd och spårbarhet i ITIL-processerna.

Kontroll	Genomförd testning	Resultat
Tester har planerats, utförts och godkänts	Test av produktionsförändringar har genomförts på ett antal olika sätt: För ett antal förändringar framgick det av statusloggen i BMC Remedy User att testning genomförts. För de förändringar som produktionssatts i samband med en planerad release (maj-, septemberreleaser) har tester för samtliga förändringar gjorts samlat. Vi har erhållit detaljerad testdokumentation för respektive release avseende systemtest nivå 1.	Av de 30 förändringar som valts att testas, noterades nio (9) fall där test ska ha genomförts men där det saknas testprotokoll. 4 av dessa har kunnat vidimeras genom att: - 2 av dessa är akuta förändringar beskrivna i RFC, - 2 är noterade som testade i leveranssedel. Resterande 5 har inte kunnat uppvisats testprotokoll för, eller förklaring till varför protokoll saknas. På grund av ovanstående utfall genomfördes en utökad testning. Av de 30 förändringar som valts att testas, noterades sjutton (17) fall där det saknas testprotokoll.
ITP har fått korrekt leveranssedel från ITA för matchning mot ändringsbegäran	För att säkerställa kontrollen efterfrågade vi leveranssedlar för samtliga förändringar.	Vi har mottagit leveranssedlar för samtliga testade förändringar.
CAB[25] har godkänt driftsättning	Innan implementering ska en förändring godkännas av CAB som har möte en gång i veckan. I de fall det är en akut incident som behöver föras in i produktionsmiljön snarast finns tre personer som ingår i CAB som kan ta beslut utanför ett CAB-möte. Här gäller samma princip som för Godkännande av programförändring (kontroll 1) för standardförändringar.	I de fall ett godkännande av CAB ska finnas har vi mottagit CAB-protokoll.

[25] Change Advisory Board (centralt ändringsråd)

Kontroll	Genomförd testning	Resultat
Ändamålsenlig ansvarsfördelning	Vi har kontrollerat i BMC Remedy User att samtliga förändringar godkänts, utvecklats, testats och driftsatts av olika personer under granskningstillfället samt i de fall det behövdes genom Henrik Ahlman som vidimerat med berörda personer.	Inga avvikelser i ändamålsenlig ansvars-fördelning har iakttagits i granskade förändringar.

4. Granskning av processer för behörighetshantering

4.1. Beskrivning av hanteringen av behörigheter

Skyddet av Försäkringskassans informationstillgångar regleras i ett regelverk för informationssäkerhet och föreskrifter angående behandling av personuppgifter. Med informationstillgångar avses både information och de IT-system som används för att hantera informationen. Regelverket utgår från myndighetens krav på tillgänglighet, riktighet, konfidentialitet och spårbarhet och härleder utifrån dessa ett antal styrande principer. För att konkretisera regelverkets innehåll har Försäkringskassan kompletterat den övergripande policyn med ett antal riktlinjer. En lista över dessa återfinns i bilaga 1.

BOA[26] är ett behörighetsregister och det övergripande verktyg som används hos Försäkringskassan för beställning och administrering av användare och behörigheter till applikationer. BOA är i sin tur kopplat till Åtkomstdatabasen som håller de aktuella behörigheterna. Dessa hämtas sedan upp av *ÄHS, TP* eller *Din Arbetsplats*[27] när en användare begär tillgång till förmånssystemen. Verktyget används för samtliga förmånssystem inom granskningens omfattning utom Tandvårdsstödet[28]. Behörighetsadministrationen består i dagsläget av ett antal manuella processer som kompletterar viss automatik i systemstöd som exempelvis BOA. Stödprocesserna utförs av 26 anställda placerade vid Försäkringskassans Behörighetsadministration i Arvidsjaur.

För att kunna logga in och få åtkomst i BOA krävs att man först loggar in på Försäkringskassans domän och Active Directory (AD), vilket görs med tvåfaktorsautentisering i form av ett smart kort kallat eID tillsammans med en PIN-kod. Genom AD-behörigheten kommer anställda enbart åt grundläggande funktioner som exempelvis e-post, hemkatalog, mappstruktur, intranät, kompetensportal, tidrapportering etcetera. Vid en fjärrinloggning, det vill säga en inloggning från annat nätverk än Försäkringskassans egna, är det också enbart dessa funktioner som kan nås och då krävs också att man ansluter med Försäkringskassans klient och tvåfaktorsautentisering motsvarande sätt.

4.2. Tilldelning av nya behörigheter

Försäkringskassan har dokumenterade riktlinjer[29] för beställning av nya IT-behörigheter 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 BOA i av den anställdes närmsta chef, eller ansvarig för projekt om behörigheten är för en extern person. Enbart dessa personer är behöriga att godkänna nya behörigheter för en anställd. I BOA finns vissa automatiska begränsningar vid en beställning av nya behörigheter. Endast personer med behörighetsroll Chef har tillgång till att lägga

[26] Systemet Behörighet, Organisation och Användare. Ett stödsystem vid Försäkringskassan för hantering av behörigheter i förmånssystemen.
[27] Det gränssnitt som handläggare använder för åtkomst till förmånssystemen.
[28] För detaljerad information om Tandvårdsstödet, se avsnitt 0
[29] Riktlinjer för informationssäkerhet – Chef, 2009:7, senast ändrad 2012-09-21.

beställningar i BOA. Utöver det kontrollerar BOA enbart att beställare och berörd anställd tillhör samma behörighetsområde[30]. Att beställaren verkligen är närmaste chef kontrolleras därefter manuellt av BA innan upplägget görs. Då HK och IT är stora behörighetsområden och väldigt många personer ingår under samma kontor, har FK infört en kompenserande kontroll där man gör en kontroll mot *Attest och delegationsordningen* för att säkerställa att den chef som beställer verkligen är behörig att beställa för aktuell person. En person kan dock inneha rollen Chef med behörighetsområde *Hela FK* vilket innebär att det inte finns några applikationsbegränsningar inom organisationen för vem han eller hon kan beställa behörigheter till.

Vid nyanställning beställer närmaste chef grundbehörighet till den nyanställde vilket innebär tillgång till dator, intranät, mail, portal etcetera. För att få tillgång till förmånssystemen krävs ytterligare en beställning av behörigheter kopplade till de arbetsuppgifter personen har. Dessa tilldelas dock inte innan den nyanställde genomgått en grundläggande säkerhetsutbildning med tillhörande godkänt provresultat. Denna kontroll görs manuellt av behörighetsadministratörerna som säkerställer att godkänt provresultat finns i *Kompetensportalen* innan behörigheten läggs upp. Behörighetsadministrationen har som önskemål att integrera exempelvis *Kompetensportalen* i BOA för att få en automatisk kontroll av utbildningsstatus. Detta är dock inget som Försäkringskassan i dagsläget har tagit beslut om att införa.

Efter det att en behörighet behandlats hos behörighetsadministrationen skickas ett kvitto till beställaren på att beställningen är genomförd om behörigheten beställts per blankett. Om den är beställd i BOA skickas inget kvitto, utan beställaren får själv gå in i BOA och kontrollera. Skulle beställningen däremot av någon anledning inte godkännas och genomföras skickas ett meddelande om avslag till beställaren via e-post.

För en nyanställd gäller också att det är närmaste chef som får eID-kortet skickat till sig samtidigt som den anställde själv får sin PIN- och PUK-kod skickat till sin folkbokföringsadress. På så sätt undviks att personer får åtkomst till Försäkringskassans nätverk och Active Directory innan exempelvis anställningen har inletts eller sekretessavtal undertecknats.

För beställning av behörigheter till konsulter gäller samma process som för en nyanställd. Eftersom konsulterna oftast arbetar i projektroller är det istället projektägaren som är behörig beställare av behörigheterna. På grund av svårigheter att kontrollera att konsulten fortfarande är anställd på konsultföretaget och arbetar för Försäkringskassan tillåts dessa roller endast åtkomst i perioder om sex månader. Efter sex månader upphör certifikatet på eID att gälla vilket hindrar användaren att kunna logga in och processen måste göras om i det fall konsulten ska ha fortsatt åtkomst. Försäkringskassan kan ställa ut ett nytt eID-kort innan det gamla slutat gälla. Vid byte ska Lokal kortadministratör (LA) först spärra och rensa det gamla kortet innan man stället ut ett nytt certifikat åt användaren.

För konsulter som bara får ha tidsbegränsade kort så börjar sexmånadersperioden att gälla så fort Behörighetsadministrationen skapat en arbetsorder i MCA-portalen[31]. När konsulten sen besöker en lokal kortadministratör (alla LA är placerade på Försäkringskassan och anställda av myndigheten) så spärrar LA det gamla kortet innan användaren

[30] Ett behörighetsområde är det kontor och kostnadsställe som den anställde tillhör.
[31] Administratörsportal för hantering av eID.

får sitt nya eID-kort. Det nya kortet gäller då i max sex månader från det att arbetsordern skapats i MCA-portalen.

Många behörighetsgrupper inom Försäkringskassan har en gruppägare. Gruppägaren meddelas i känsliga fall när en behörighetsbeställning lagts för gruppen. Vid ett upplägg av behörighet till en grupp innefattande känslig information eller till ett system som endast ett begränsat antal anställda ska ha tillgång till kan gruppägaren lägga in veto i behörighetsärendet. Detta dubbelkommando innebär att en behörighetsbeställning kan avvisas trots påskrift från närmaste chef om gruppägaren inte anser att den anställde behöver eller bör ha behörighet till systemet.

Vid uppläggning av nya behörigheter görs också en kontroll av *Behörighetsadministrationen* att medarbetaren inte innehar behörigheter som inte får kombineras med den nya behörigheten. Man kontrollerar även att personen arbetar inom exempelvis rätt verksamhets- eller behörighetsområde för att vara godkänd för behörigheten i enlighet med Säkerhetsstabens beslut[32]. Dessa kontroller är dock inte heltäckande för samtliga förmånssystem ingående i granskningen, men BA har inlett ett arbete med att se över dessa kontroller under 2014. BA upplever dock vissa utmaningar med att få stöd avseende vilka kombinerade behörigheter som är känsliga inom Förmånssystemen. BA anser sig vara en utförandeorganisation och behöver få profiler och roller beskrivna för sig tillsammans med verksamhetens underlag för känsliga kombinationer. Detta går också i linje med riktlinjerna[33] där det framgår att *Roller fastställs av HR. För roller inom handläggning bidrar kundkanaler eller Försäkringsprocesser med nödvändigt innehåll för att behörighetsprofiler ska kunna realiseras på rätt sätt.* På samma sätt uppfattar BA att verksamheten saknar en löpande uppföljning av vilka roller och profiler som är aktuella då man inte får någon fortlöpande återkoppling.

Användarbehörigheter för Tandvårdsstödet hanteras utanför BOA då verktyget inte är kompatibelt med SAP som Tandvårdsstödet använder. Istället beställs behörigheter till Tandvårdsstödet genom blanketter. Dessa är elektroniska inom Försäkringskassan och i pappersform för externa parter, det vill säga tandläkare. Pappersblanketterna görs därefter om till elektronisk form av en tandvårdsstödshandläggare där man signerar blanketten med sitt personliga certifikat(eID) för att säkerställa beställarens identitet. Blanketten skickas därefter till *Behörighetsadministrationen* med e-post till BA:s funktionsinkorg för hantering och manuella kontroller enligt ordinarie rutin. För interna behörigheter görs en chefskontroll av *Behörighetsadministrationen* med hjälp av BOA eller Attest- och delegationsförteckningen för att säkerställa att beställningen gjorts av medarbetarens chef, samt manuella kontroller på samma sätt som för BOA-beställningar. För tandläkare i Tandvårdsstödet kontrolleras att den handläggare vid FK som skickat vidare beställningen till behörighetsadministrationen har handläggarbehörighet i Tandvårdsstödet.

I övrigt används blanketter för de system i granskat scope endast för ansökan om behörigheter för registervård, vilket då hanteras enligt ordinarie rutin men med utökad kontroll genom kontroll mot BOA där man kontrollerar att chef är behörig beställare.

---

[32] beslut-120412-dnr-16588-2012-otillatna-behorighetskombinationer
[33] Riktlinjer för informationssäkerhet - Behörighetsadministration v1.2

Inom Försäkringskassan finns handläggare med behörighet att handlägga ärenden rörande personer med skyddade personuppgifter, s.k. SID[34]-handläggare. Vilka som är SID-handläggare ska enligt riktlinjerna enbart vara känt av chef på högre nivå, exempelvis kontorschef. Generaldirektören för Försäkringskassan har under 2012 ålagt alla chefer att göra en prövning av samtliga SID-handläggare och man har nu minskat sitt antal SID-chefer med cirka 65 procent av tidigare antal.

En manuell kontroll av SID-beställningar ska alltid göras av Behörighetsadministrationen, där man kontrollerar att det är en behörig SID-chef som gör beställningen. Om behörighets beställs för SID-åtkomst av person som inte är behörig beställare så är rutinen att Behörighetsadministrationen vid FK 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.

4.2.1. Priviligierade (höga) IT-behörigheter

Processerna för behörighetshantering av höga IT-behörigheter hanteras inte av Behörighetsadministrationen, utan ligger inom Försäkringskassan IT. Istället sker upplägg och borttag av behörigheter genom informella processer inom respektive teknikområdesgrupp. Dessa informella processer avseende privilegierade IT-behörigheter är inte specificerade eller dokumenterade, vilket gör att de myndighetsövergripande riktlinjer som existerar med andra ord inte efterföljs.

Ett projekt pågår dock att införa en automatiserad behörighetshantering med hjälp av ett IAM-verktyg[35] vilket beräknas vara infört till sommaren 2014. Syftet med projektet är att effektivisera administrationen. Idag är det krångligt för enhetschefer att beställa behörigheter, men systemet ska även vara ett stöd i bedömning vid tilldelning av behörigheter. Idag har de som jobbar inom IT högre behörigheter än vad som är nödvändigt i deras roller på grund av att man inte har systemstöd för tilldelning och bedömning.

De huvudsakliga målen med den nya lösningen är:

- Renodla mot tre plattformar där ett nytt Datacenter ska vara infört 2015.
- Införande av PAM[36]-lösning där man med största sannolikhet kommer att gå mot en färdig hyllprodukt som stödjer hela processen för tilldelning av behörigheter.
- Städning för att få ordning på de gamla myndighetsbehörigheterna samt göra en genomgång av samtliga (access-)grupper med koppling till IT-infrastruktur.

För att skapa enhetlighet och struktur inom behörighetshanteringen fram till införandet av IAM-verktyget hade, enligt föregående års granskning, Försäkringskassan för avsikt att innan årsskiften 2012/2013 införa en interimistisk lösning i form av dokumenterade manuella rutiner. Detta har man valt att frångå och arbetar istället direkt mot införandet

[34] Skyddad identitet.
[35] Identity and Access Management, avser alla policys, processer, rutiner och system som stöder en organisation i hanteringen av åtkomst till information och funktionalitet.
[36] Privileged Access Management.

av IAM-lösningen. Man är vid granskningens genomförande i uppstartsfasen av genomförandeprojektet som beslutades 1 oktober 2013.

4.3. Borttagning av behörigheter

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

4.3.1. Avslutad anställning

Vid avslutad anställning tas eID-kortet tillbaka från den anställde vilket innebär att han/hon inte längre har fysisk access till lokalerna eller 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. Om borttaget av behörigheter ligger längre fram i tiden så läggs de upp i en separat inbox i Outlook/Exchange när de hanteras av BA och taggas med färg/datum och bevakas, men det finns inga automatiserade kontroller för tidsbestämt borttag av behörigheter. Därefter tas även behörigheten bort från systemen inom en 30-dagarsperiod. Detta sker genom en kompenserande kontroll där Behörighetsadministration tar del av lönelistor för Försäkringskassan via Statens Service Center, vilka sedan jämförs med aktuella behörigheter och där man avslutar de som inte finns representerade på lönelistan. Användarkonton sparas av Försäkringskassan i tio år innan de raderas från Active Directory och systemen för att behålla spårbarhet.

4.3.2. Ändrad anställning

Vid en förändrad anställning eller geografisk flytt av en anställd gäller att den anställdes behörigheter ska ändras till grundbehörighet. Enligt gällande riktlinjer[37] 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. Detta för att närmsta chef alltid ska vara den som begärt de behörigheter som är aktuella för den innehavda rollen. I praktiken har BA fått ok av Säkerhetsstaben att tillåta att det endast är den nya chefen som hanterar alla behörigheter den anställde ska ha i sin tjänst. Detta finns inte beslutat och uppdaterat i riktlinjerna för informationssäkerhet, men är en muntlig överenskommelse mellan BA och Säkerhetsstaben.

Vid begäran av nya behörigheter till befintlig användare skickas en totallista till den nye chefen med medarbetarens existerande behörigheter som orientering. Detta bidrar till en ökad sannolikhet att fånga upp behörigheter som inte längre ska finnas i systemet, då även den nye chefen kan flagga för inaktuella behörigheter.

[37] Riktlinje informationssäkerhet – Chef, 2009:07.

4.4. Periodisk genomgång av behörigheter

Enligt Försäkringskassans *Riktlinjer för Informationssäkerhet – Chef (2009)* ska en total uppföljning av samtliga användarbehörigheter genomföras en gång per år för att säkerställa att behörigheterna är behovsanpassade baserat på arbetsuppgifter. Ansvaret för att detta utförs ligger på myndighetens *Verksamhetsstöd (VS)* som kravställer *Behörighetsadministrationen* att upprätta och distribuera listor över behörigheter till respektive chef som förväntas granska dessa.

Det är alltid närmsta chef som har ansvaret för sina medarbetares behörigheter och att dessa är roll- och behovsanpassade. Listorna med information gällande vilka medarbetare som innehar behörigheter i förmånssystemen hämtas från ett antal system, exempelvis från *Tandvårdsstödet* och från databasen *Åtkomstkontroll*. Listorna distribueras sedan ut till berörda chefer genom BA:s försorg. Utifrån detta underlag är det chefens ansvar att kontrollera vilka behörigheter som finns med hjälp av bland annat BOA, samt dokumentera att genomgång genomförts. Under granskningen har det framkommit att listorna uppfattas som svårtolkade för cheferna, då de innehåller tekniska utdrag ur system och inte är självförklarande eller har tillräcklig beskrivning i utskicket. Detta gör det svårt för cheferna att egentligen förstå vilka faktiska behörigheter som deras personal har, utan kontrollen blir mer av karaktären att jämföra tilldelade behörigheter mellan personal. Skulle felaktigheter upptäckas under genomgången ska chefen därefter vidta nödvändiga åtgärder och säkerställa att behörigheterna rättas till. För projektanställda är det projektägaren som har ansvaret att göra genomgången och se till att deltagarna har rätt behörigheter.

För privilegierade och känsliga behörigheter (SID med flera) säger riktlinjerna[38] att genomgång ska genomföras med tätare tidsintervall, normalt var tredje månad men i praktiken genomförs den ungefär en gång per halvår. Övriga särskilda priviligierade behörigheter, som exempelvis systemadministratör eller databasadministratör vid IT med tillgång till känslig information, genomförs det med inom egen grupps försorg och utan gemensam uppföljning och kontroll.

Det finns i dagsläget ingen dokumenterad uppföljning på att den periodiska genomgången verkligen genomförs av samtliga chefer. Chefen ska efter genomförd genomgång signera listan över användare samt spara denna. Utifrån det genomför Säkerhetsstaben, som har en reviderande funktion för uppföljning, stickprovskontroller bland cheferna för att kontrollera rutinens efterlevnad.

En sådan granskning genomförs under sista kvartalet 2013, men vid tillfälle för granskningen har underlaget inte hunnit samlas in och sammanställts. Säkerhetsstaben har då valt att göra ett urval på 10 % av de berörda cheferna och genom en webbenkät ställer man frågan till cheferna om de genomfört granskningen. Då stickprovet genomförs i formen av en enkät kan det ge en indikation på brister, men inte ett svar på vilken faktisk nivå av genomförda kontroller FK har. Detta är första gången man gör denna typ av kompenserande kontroll. Fortsättningsvis är målet att denna kontroll ska införlivas i en den befintliga process som BA äger, genom att cheferna istället ska returnera de utskick som görs av BA och på så sätt ska en mer kontrollerad uppföljning skapas.

---

[38] Riktlinje för informationssäkerhet – Behörighetsadministration 2010:5, samt Riktlinjer för informationssäkerhet – Chef 2009:7.

4.5. Spårbarhet avseende behörighetsförändringar

I BOA finns en god spårbarhet då detta lagras direkt i systemet genom inloggningsinformation. Spårbarhet i BOA ger följande:

- Beställd av
- Beställt klockslag och tidsnummer
- Åtgärd
- Åtgärdad av (användar-ID och namn)
- Åtgärdat klockslag och tidsnummer

Det finns även en spårbarhet av behörighetshantering med blanketter avseende vem som har sparat ner blanketten på disk där den arkiveras på gemensam yta. När blanketter sparats ner på disk kan de inte flyttas eller raderas utan administratörsrättigheter.

Det finns en rutin/lathund för arkivering av behörighetsbeställning per blankett. För blankettbeställningar så skickar BA alltid en kvittens till den beställande chefen och i meddelande meddelas bland annat användar-ID för en ny användare. Avslagna blanketter arkiveras dock inte i samma struktur som genomförda beställningar, utan BA skickar e-post till sökande chef med blankett som innehåller motiv för avslag. När e-posten skickats sparas det i en särskild mapp i Outlook/Exchange för avslagna ärenden.

4.6. Förändringar av behörighetsprocessen

BA har under 2013 tagit fram en uppdaterad behörighetsprocess[39] vilken är beslutad och gäller från den 4 november 2013. Den största delen av processen är densamma som tidigare har gällt för Försäkringskassan, men den har inte varit dokumenterad som en stödprocess. I den nya processen har man tillfört pkt 2.5 Attest- och delegationsförteckning där man även tillfört nya blanketter samt förtydligat administration av behörigheter för *Chef*.

BA har tagit fram en blankettmall som listar allt som ingår i beställningen, inklusive chefsrollen i BOA. Vid beställning av chefsroll enligt blankett läggs det sedan in av BA i BOA. I blanketten kan man även välja om det är tillfälligt chefbeställning. Detta innebär att man definierat grundbehörighet för chef och det blir samma för alla vilket förenklar beställningsförfarandet. Vidare har man kopplat attest- och delegationsordningen till behörighet för kontrollera rätt att besluta om behörigheter i system. Chefer kopplas nu tydligare till ett kostnadsställe. Idag kan man därför inte längre beställa chefsrollen direkt i BOA som tidigare, då områdeschefer beställde för enhetschefer. Nu sker det på ett smidigare och på ett mer kontrollerat sätt genom blanketten.

Den chef som får behörigheter att beställa(besluta) behörigheter ser, och kan endast beställa till, den personal som ligger på samma sitt kostnadsställe som chefen.

Vidare arbetar Behörighetsadministrationen även på att förbättra den kvartalsvisa uppföljningen. Det kommer då att synas vilka behörigheter som finns i BOA i de Excel-listor som skickas ut för granskning av chefer. Det är dock inte beslutat om cheferna

[39] Hantering av utökade behörigheter – Stödprocess v1.0 2013:2

kommer att kunna beställa borttag av behörigheter på denna blankett genom att markera borttag och returnera listan, eller om de fortsatt ska göra det själva i BOA eller via blankett.

4.7. Test av kontroller i processen för hantering av behörigheter

4.7.1. Testade kontroller

Vår testning av kontroller rörande hantering av behörigheter har endast fokuserat på upplägg av nya behörigheter i samtliga förmånssystem då övriga kontroller inom behörighetshantering inte varit möjliga att testa. Den anställdes närmsta chef ansvarar för att återkalla behörigheter vid ett byte av arbetsuppgifter. För att fånga upp risken att detta inte görs förlitar sig Försäkringskassan på den periodiska behörighetskontroll som chefer vid myndigheten utför. Eftersom det inte finns något krav på att chefer återkopplar efter utförd kontroll finns det ingen möjlighet att följa upp att samtliga chefer har utfört kontrollen, vilket skulle utgöra den spårbarhet som krävs för testning av kontrollens operationella effektivitet. Underlaget från Säkerhetsstaben kompenserande kontroll är vid granskningens genomförande ej färdigställt och grundar sig på en enkät, vilket inte kan ses tillräckligt för att säkerställa effektivitet i chefers genomförda kontroller.

Vid avslutad anställning har en tidigare anställd inte längre tillgång till det smarta kort som krävs för inloggning i Active Directory. Då åtkomsten till förmånssystemen är kopplad till behörigheten i Active Directory minskar risken markant att personer som inte längre arbetar på myndigheten har fortsatt åtkomst till förmånssystemen eller andra system.

4.7.2. Urval av behörigheter

För att genomföra testningen erhölls listor på samtliga behörigheter som ändrats under perioden 2013-01-01 till 2013-11-26 för alla förmånssystem inom ramen för granskningarna på Försäkringskassan och Pensionsmyndigheten. Majoriteten av systemen hanteras i verktyget för behörighetshantering BOA, där bland annat beställningar läggs men lagras sedan i databasen Åtkomstkontroll. Behörighetsinformationen hämtas därefter vid en inloggning av det handläggarsystem man använder (ÄHS, TP m.fl.). Från Åtkomstkontroll kommer den lista över behörigheter varifrån vi gjort urvalet av behörigheter för kontrolltestning. Tandvårdsstödet hanteras separat i SAP vilket medfört att en särskild lista genererats därifrån för dessa behörighetsroller.

Utifrån dessa listor bestående av ca 49 500 förändrade behörigheter i BOA och ca 16 700 förändrade behörigheter i Tanden, valdes totalt 60 behörighetsförändringar[40] ut som stickprov för närmare granskning. För samtliga utvalda förändringar begärdes sedan beställning och godkännande in från Behörighetshanteringen.

4.7.3. Resultat

Vi har mottagit dokumentation för nästintill samtliga förändrade behörigheter i samtliga förmånssystem. Detta har antingen skett genom utdrag från behörighetsverktyget BOA eller genom inskickade blanketter för Tanden (SAP).

[40] 30 stycken från varje lista av BOA respektive Tanden.

Den stora majoriteten av urvalet har hanterats enligt rutin och kan styrkas antingen genom dokumentation eller i system.

De brister som identifierats är i hanteringen av tandvårdsystemet Tanden (SAP). Fyra (4) raderade behörigheter går ej att spåra till beställning, men dessa utgör en mindre risk då behörigheterna raderats. Två (2) behörigheter kan ej styrkas:

- Den ena går ej att spåra med beställningsblankett, och vi har inte kunnat få fram anledningen till att den inte finns.
- Den andra beror på att vi inte kan spåra beställaren i den nu gällande Attest- och delegationsordningen. Beställaren är känd av personalen vid BA och har arbetat som chef vid kontoret där personen som fått behörighet arbetar. Detta gör det möjligt att beställaren fanns med i Attest- och delegationsordningen vid beställningstillfället och då var behörig.

5. Identifierade iakttagelser och förbättringsområden

5.1. Inledning

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

5.1.1. 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.

5.1.2. Riskklassificering för samtliga identifierade iakttagelser

I följande tabell presenteras riskerna kopplade till identifierade iakttagelser:

#	Iakttagelse	Risk	Risknivå
5.2	Systemgenererade listor över applikations-förändringar kan för närvarande inte produceras	Avsaknad av fullständiga listor över applika-tionsförändringar 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
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 produktionsmiljön.	Medel

#	Iakttagelse	Risk	Risknivå
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
5.5	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
5.6	Otillräckliga automatiska kontroller vid behörighets-beställning 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
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
5.8	Ingen spårbarhet i förändringar av Attest- och delegations-ordningen	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
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
5.10	Informella rutiner och otydlighet kring privilegierade 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
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

#	Iakttagelse	Risk	Risknivå
0	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
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

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

5.2. Systemgenererade listor över applikationsförändringar kan för närvarande inte produceras

5.2.1. Iakttagelse

Vid vår granskning noterade vi att Försäkringskassan under 2011 har implementerat ett CMDB[41]-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.

5.2.2. 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.

5.2.3. Rekommendation

Vi rekommenderar 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.

5.2.4. Status

Kvarstående iakttagelse sedan tidigare granskning.

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

5.3. Osäker ändringsrutin för standardändringar i COBOL

5.3.1. 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 förhands-godkännande. 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. Testningen av dessa COBOL-ändringar genomförs av resurser inom VO Applikation och verifieras efter överlämning av ändringsplanerare innan driftsättning i produktion.

5.3.2. 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.

5.3.3. Rekommendation

Vi rekommenderar 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.

5.3.4. Status

Kvarstående iakttagelse sedan tidigare granskning.

5.4. Bristande tydlighet i hur nödvändiga testnivåer fastställs

5.4.1. 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.

5.4.2. 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.

5.4.3. Rekommendation

Vi rekommenderar 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.

5.4.4. Status

Kvarstående iakttagelse sedan tidigare granskning.

5.5. Bristande spårbarhet gällande testning av applikations-förändringar

5.5.1. 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.

5.5.2. 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.

5.5.3. Rekommendation

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

5.5.4. Status

Kvarstående iakttagelse sedan tidigare granskning.

5.6. Otillräckliga automatiska kontroller vid behörighets-beställning i BOA

5.6.1. 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. Dessa täcker dock inte samtliga förmånssystem.

5.6.2. Risk

Medel	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.

5.6.3. Rekommendation

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.

5.6.4. Status

Kvarstående iakttagelse sedan tidigare granskning.

5.7. Avsaknad av systemstöd för tidsbestämda borttag av behörigheter och konton

5.7.1. Iakttagelse

Borttag av behörigheter ska beställas av chef direkt i BOA eller per blankett för system utanför BOA. Om borttaget av behörigheter ligger längre fram i tiden än vid tidpunkten för beställning, så läggs de upp i en separat inbox i Outlook/Exchange och taggas med färg/datum och bevakas manuellt av Behörighetsadministrationen. Det saknas automatiserade kontroller för tidsbestämt borttag av behörigheter, där BA i gränssnittet Identity Manager mot AD kan tidsbestämma när användarkontot ska låsas.

5.7.2. Risk

Låg	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.

5.7.3. Rekommendation

Vi rekommenderar Försäkringskassan att utreda möjligheterna att införa systemstöd för att vid beställning av borttag av behörigheter kunna i Identity Manager (Active Directory) eller BOA med tidsbegränsning kunna styra borttag av behörigheter eller låsning av konto.

5.7.4. Status

Ny iakttagelse identifierad under denna granskning.

5.8. Ingen spårbarhet i förändringar av Attest- och delegationsordningen

5.8.1. Iakttagelse

Vid granskningen och testningen av behörighetsförändringar i förmånssystemen vid Försäkringskassan har vi tagit del av Attest- och delegationsordningen, som används vid kontroller vid behörighetsförändringar för att säkerställa behörig beställare (Chef). Vid testning av behörighetsförändringar har det framkommit att det inte finns spårbarhet avseende förändringar i dokumentet då den sparas som en Excelfil.

5.8.2. Risk

Låg	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.

5.8.3. Rekommendation

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

5.8.4. Status

Ny iakttagelse identifierad under denna granskning.

5.9. Avsaknad av säkerhetsprövning för personal med höga IT-behörigheter

5.9.1. Iakttagelse

Genom intervjuer vid Försäkringskassans IT så har det framkommit att viss personal har tillgång till känslig information(t.ex. SID-information) genom systemadministrativa rättigheter i sina roller som exempelvis utvecklare eller databasadministratör. Det görs dock inte rutinmässigt bakgrundskontroll enligt formellt fastställd rutin eller process, på det sätt som SID-behörigheter kontrolleras. Det är dock något som man belyst som ett behov inom Försäkringskassan IT under det gångna året.

Detta är även krav som Pensionsmyndigheten har i ställt i sina samarbetsavtal[42], där personal vid Försäkringskassan som har arbetsuppgifter enligt vissa specificerade kriterier ska genomgå säkerhetsprövning. Det berör bland annat områden som relaterar till höga IT-behörigheter.

5.9.2. 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.

5.9.3. Rekommendation

Vi rekommenderar 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 myndigheter.

5.9.4. Status

Ny iakttagelse identifierad under denna granskning.

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

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

5.10.1. Iakttagelse

IT pekas ut som ansvarig för hantering av IT-behörigheter i Försäkringskassans riktlinje för informationssäkerhet[43] avseende 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 de inlett ett projekt för implementering av ett IAM-system för hantering av behörigheter under 2013 enligt föreslagen utvecklingsplan. IAM-systemet med behörighetsprocess 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.

5.10.2. 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. 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.

5.10.3. Rekommendation

Ett arbete pågår med att implementera ett IAM-system för ökad kontroll av behörighetshantering 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.

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

5.10.4. Status

Kvarstående iakttagelse sedan tidigare granskning.

5.11. Mindre brister i hantering av SID-behörigheter

5.11.1. 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 därför infört en kompenserande detektiv kontroll där myndigheten månatligen går igenom tilldelade SID-behörigheter och återrapporterar dessa till utpekad SID-chef. Denna kontroll är positiv och tillämplig, men kan inte ses som tillräcklig då det skulle kunna innebära att SID-behörigheter ges ut felaktigt upp till en månads tid.

5.11.2. Risk

Medel	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.

5.11.3. 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 konsekvenser för enskild person rekommenderar vi Försäkringskassan att hantera felaktig och obehörig beställning av SID-behörighet som en säkerhetsincident.

5.11.4. Status

Kvarstående iakttagelse sedan tidigare granskning.

5.12. Brister i uppföljning efter periodisk genomgång av behörigheter

5.12.1. Iakttagelse

Försäkringskassan genomför periodiska genomgångar av samtliga behörighetsroller minst en gång om året genom utskick till ansvariga chefer i verksamheten. Vi har dock noterat att man i samband med denna genomgång inte säkerställer att samtliga chefer gjort vad som ålagts dem. Man har valt att inte samla in dokumentation som visar att genomgången är genomförd. Istället tar säkerhetsstaben efter varje genomgång ett stickprov bland cheferna där man kontrollerar att genomgången genomförts. Då stickprovet genomförs i formen av en enkät kan det ge en indikation på brister, men inte ett svar på vilken faktisk nivå av genomförda kontroller FK har.

Vidare har vi noterat att listorna uppfattas som svårtolkade för cheferna, då de innehåller tekniska utdrag ur system och inte är självförklarande eller ej har tillräcklig beskrivning. Detta gör det svårt för cheferna att förstå vilka faktiska behörigheter som deras personal har, utan kontrollen blir mer av karaktären att jämföra tilldelade behörigheter mellan personal.

5.12.2. Risk

Låg	Att inga återkopplingskrav finns på chefer efter periodiska behörighets-genomgångar 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.

5.12.3. Rekommendation

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.

5.12.4. Status

Kvarstående iakttagelse sedan tidigare granskning.

5.13. Brister i regelbunden uppföljning av särskild, priviligierad behörighet

5.13.1. Iakttagelse

Försäkringskassan genomför periodiska genomgångar av samtliga behörighetsroller minst en gång om året genom utskick till ansvariga chefer i verksamheten. Enligt fastställda riktlinjer ska periodiska genomgångar av särskild, priviligierad åtkomsträtt granskas med tätare intervall, normalt var tredje månad. Detta görs för SID-handläggare, men sker inte generellt för exempelvis IT-behörigheter som Systemadministratörer eller databas-administratörer med tillgång till känslig information.

5.13.2. Risk

Medel	Att periodiska behörighetsgenomgångar inte generellt genomförs för särskilda, priviligierade 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.

5.13.3. Rekommendation

Vi rekommenderar Försäkringskassan att säkerställa periodiska behörighetsgenomgångar för särskilda, priviligierade behörigheter inom IT.

5.13.4. Status

Ny iakttagelse identifierad under denna granskning.

Bilaga 1 – Metod

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

Omfattning

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 Försäkringskassan
  - Övergripande beskrivning av genomförande
  - Övergripande identifiering av nyckelpersoner för informationsinsamling
  - Förberedande arbete inför granskning
- På-plats-granskning
  - Intervjuer
  - Visuella granskningar
  - Stickprovtestning
- 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 roller har intervjuats/bidragit inom ramen för granskningen:

Namn	Roll
Anna-Karin Englund	Gruppledare Tandvårdsstödet, ITA
Henrik Ahlman	Områdeschef projektkontor, ITA.
Jan Wikström	Projektledare IT-behörigheter och IAM, ITP
Jenny Stenfors	Verksamhetsutvecklare, ESU
Joakim Lundberg	Verksamhetsspecialist, Behörighets-administration
Kalif Hassan	IT-arkitekt informationssäkerhet, ITA
Kerstin Wiklund	Verksamhetsutvecklare, ESU
Kjell Pettersson	IT- arkitekt, ITA
Lena Sandh	Verksamhetsområdeschef, ESU
Mats Svärdsudd	IT-säkerhetschef
Michael Sjölén	Områdeschef Process och Kvalité, ITP.
Peter Sahlin	Verksamhetsområdeschef, ITK
Robert Tencic	Infrastrukturarkitekt, ITP
Soumi Seppo	Säkerhetsspecialist, Säkerhetsstaben
Thomas Danielsson	Processansvarig releaseprocessen, ITP

Namn	Roll
Tomas Isakas	Systemutvecklare (SAP), ITA
Tomas Stenlund	Områdeschef, Behörighetsadministration
Ulrika Engberg	Verksamhetsutvecklare projektkontoret, ITA
Vera Bylund	Enhetschef projektkontoret, ITA
Örjan Lindgren	Verksamhetsspecialist, Behörighetsadministration
Maria Bolund	Projektkontoret, Change Manager

Följande dokument har använts som stöd för granskningens resultat:

Dokument	Version
Hantering av utökade behörigheter – Stödprocess	v1.0
Riktlinjer för informationssäkerhet – Chef	v2.4
Riktlinjer för informationssäkerhet - Behörighetsadministration	v1.2
Riktlinjer för informationssäkerhet - Medarbetare	v2.4
Vägledande principer för samarbetet mellan FK och PM	v2.0
Beslut otillåtna behörighetskombinationer	2012-05-04
Hantering av utökade behörigheter – Stödprocess, 2013:2	v1.0
Test på Försäkringskassan FK RUP, Rev E	2009-10-01
Uppdragsflödet_flödesbilder PD7	
Försäkringskassans Utvecklingsprocess - Processbeskrivning och processroller	2010-05-14
Ändringshanteringsprocessen	2010-06-23
Godkännandekriterier ITP FebR	2013 RevA

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. De testade kontrollerna ska tillämpas oberoende av applikation, vilket innebär att testningen utgör ett underlag även för applikationer som inte finns med i urvalet.

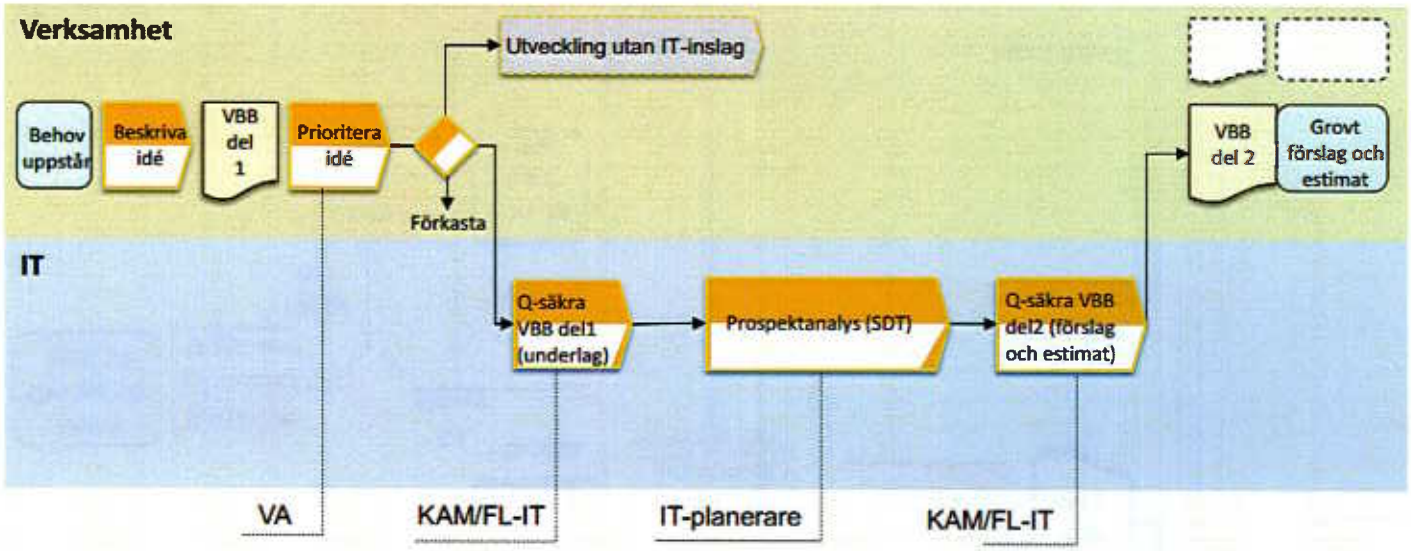
Applikationer	
Utbetalningssystemet	Sjuk- och aktivitetsersättning
Arbetsskadelivränta	Yrkesskadelivränta
Vårdbidrag	Tillfällig föräldrapenning
Föräldrapenning	Sjukpenning
Bostadsbidrag	Barnbidrag
Underhållsstöd	Bilstöd
Familjebidrag till värnpliktiga	Assistansersättning
Handikappersättning	Etableringsersättning
Tandvårdsstödet	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 – Försäkringskassans processer för uppdragsplanering

Fas 1[44]: Från behov till grovt förslag och estimat



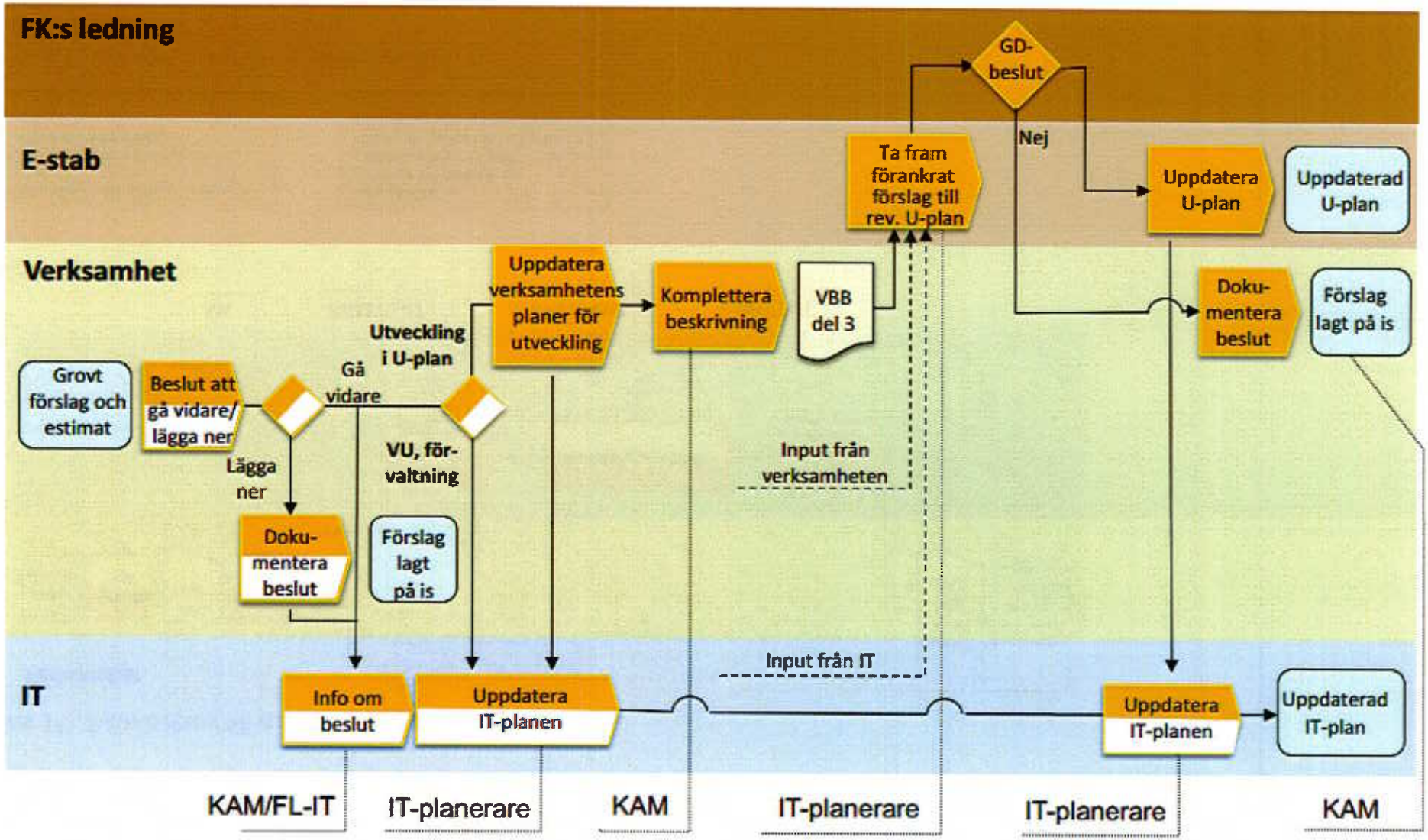
Gula flödesrutor gäller utveckling i U-planen.
Vita flödesrutor gäller Mindre vidareutveckling (MVU).

VU & Förvaltning
FL-IT hanterar de operativa arbetsuppgifterna i stället för KAM; KAM är informerad och tar sitt ansvar enligt rollbeskrivning Objektägare IT

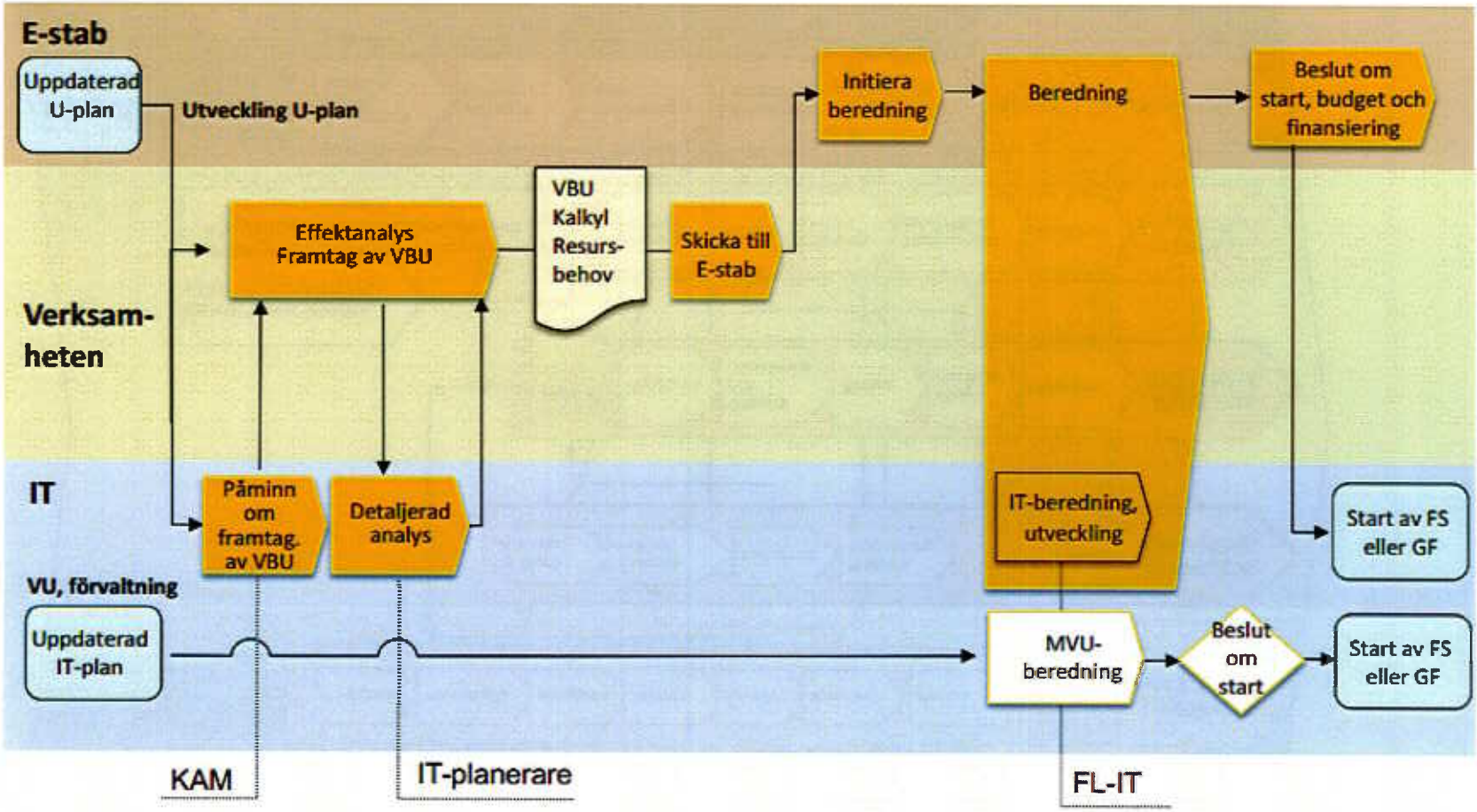
Fotnot: **IT-planerare** faciliteras av personer från Uppdragsplanering (ITA) och Tjänsteintroduktion (ITP)

[44] KA heter numera KAM.

Fas 2: Från grovt förslag och estimat till uppdaterad U-plan och IT-plan

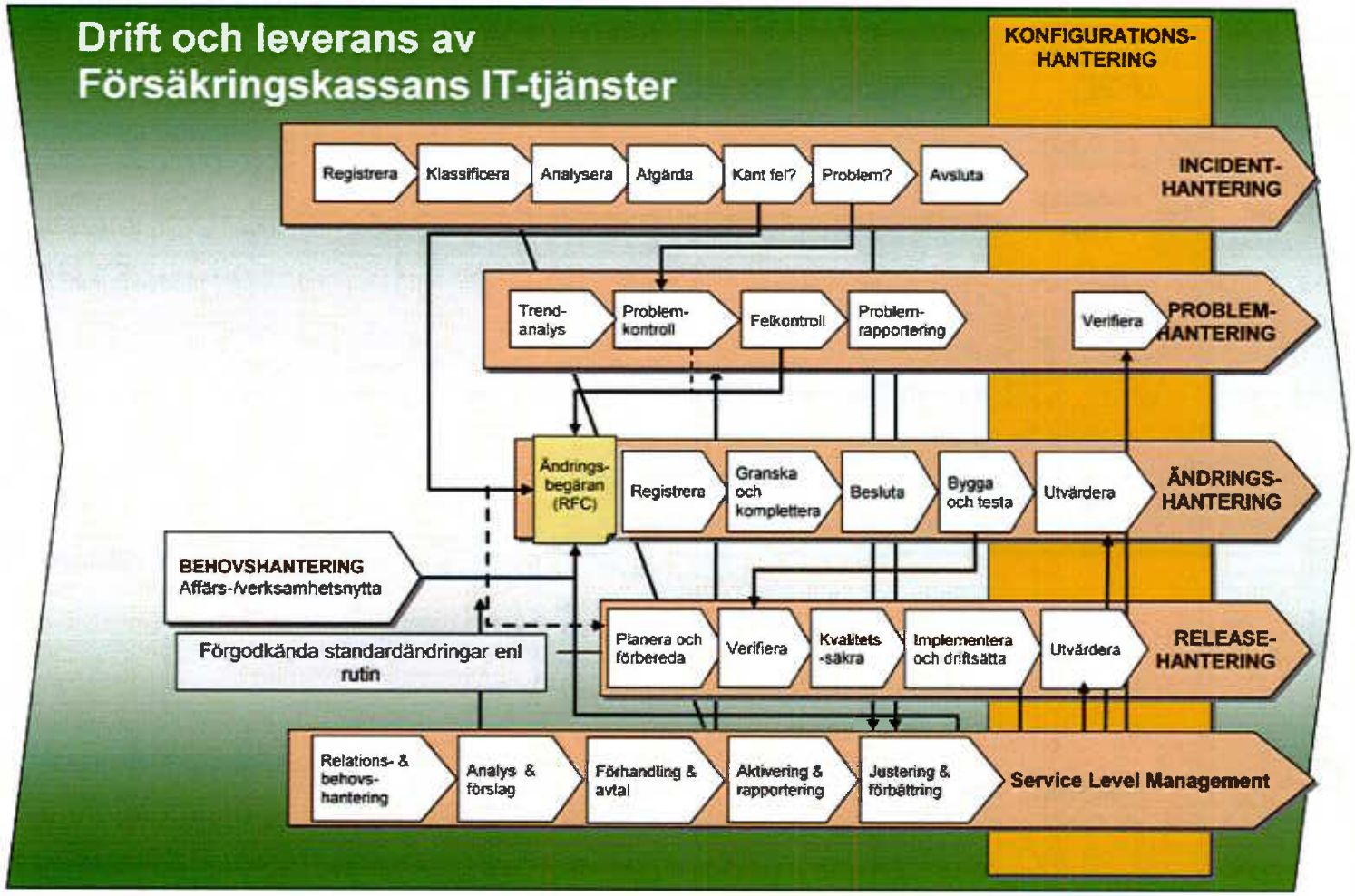


Fas 3: Från uppdaterad Utvecklingsplan till IT-beredning



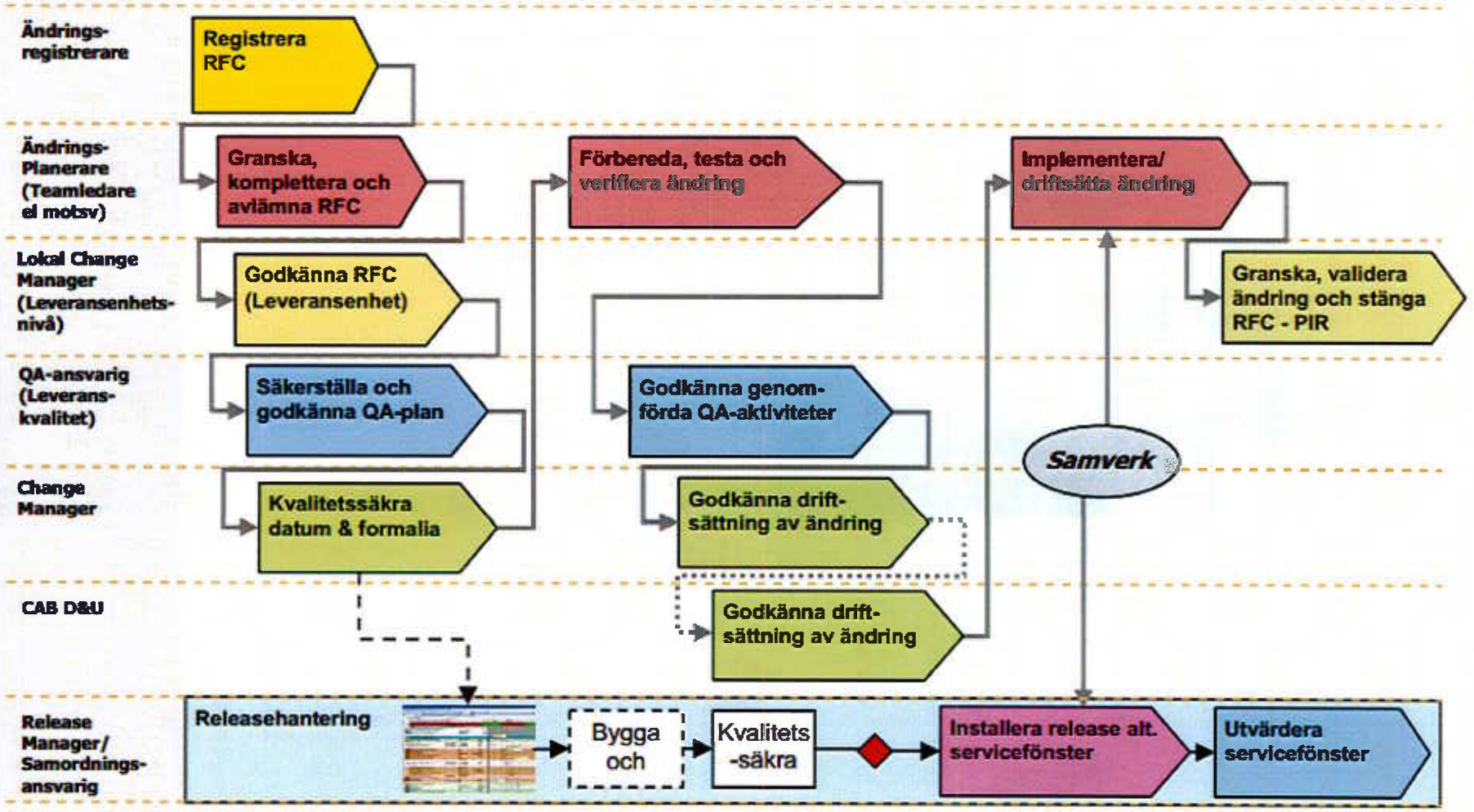
För prospekt där både FS och GF ska göras loopar man om endast fas 3 efter FS är genomförd.
Efter genomförd FS uppdateras IT-planen. Därefter initieras framtagande av VBU för GF.

Bilaga 3 - Försäkringskassans processer för leverans av IT-tjänster45

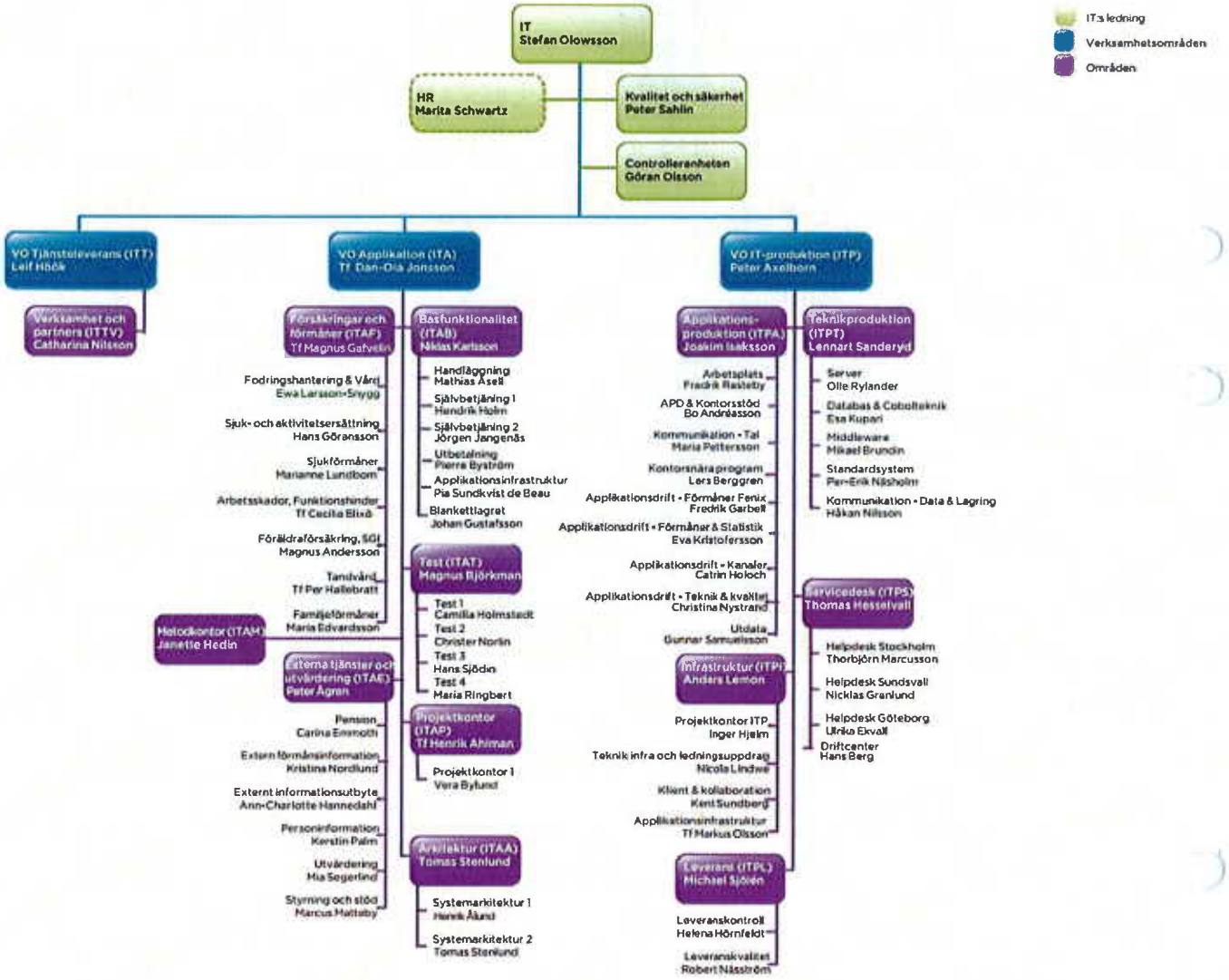


[45] Samtliga bilder i bilaga 3 är tillhandahållna av Försäkringskassan.

Processerna för ändrings- och releasehantering ur ett rollperspektiv:



Bilaga 4 Försäkringskassans IT-organisation[46]



[46] Denna organisationskarta är tillhandahållen av Försäkringskassan 2013.