RIKSREVISIONEN

Granskning av Försäkringskassans interna styrning och kontroll av informationssäkerheten

Revisionsrapport

ISBN 91 7086 075 0

Tryck: Riksdagstryckeriet, Stockholm 2006

Revisionsrapport

RIKSREVISIONEN

Till
Försäkringskassan

Datum 2006-04-28
Dnr 32-2005-0655

Försäkringskassans interna styrning och kontroll av informationssäkerheten

Riksrevisionen har som ett led i den årliga revisionen av Försäkringskassan granskat Försäkringskassans arbete med informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa Försäkringskassans uppmärksamhet på i denna revisionsrapport.

Riksrevisionen önskar information senast 2006-05-29 med anledning av våra iakttagelser i denna rapport.

Revisionschef *Karin Holmerin* har beslutat i detta ärende. Biträdande revisionschef *Stefan Gollbo* har varit föredragande. Revisionsdirektör *Björn Undall* och revisionsdirektör *Bengt EW Andersson* har medverkat vid granskningen.

Karin Holmerin

Stefan Gollbo

För kännedom
Socialdepartementet

Innehåll

Sammanfattning

Post- och telestyrelsens incidentcentrum Sitic konstaterar att nära en tredjedel av alla offentliga organisationer har utsatts för någon form av allvarligt dataintrång eller virusangrepp. Angreppen blir alltmer ”professionella”. Samtidigt lägger myndigheterna ut alltmer av sin verksamhet på Internet i form av elektroniska tjänster. Myndigheterna behöver därför arbeta med att skydda sin information, IT-miljö och verksamhet. Det är både svåra frågor att hantera, inte minst att synliggöra nyttan av säkerhet i verksamheten, och ofta resurskrävande ju mer komplicerad verksamheten och IT-miljön är. Det är mot denna bakgrund som Riksrevisionen har ökat sina insatser i granskningen av informationssäkerhet inom staten. Denna granskning gäller Försäkringskassans arbete med sin informationssäkerhet.

Vad menas med informationssäkerhet?

Informationssäkerhet handlar om att rätt information ska finnas tillgänglig och att den inte ska kunna förvanskas eller vara möjlig att komma åt för obehöriga. Det ska också vara möjligt att spåra bakåt vem som använt informationen och därvid särskilt om information manipulerats.

Riksrevisionen har i sin granskning utgått från en internationell standard för informationssäkerhetsarbete (SS-ISO/IEC 17799), som beskriver ett ledningssystem för informationssäkerhet, den s.k. LIS-standarden, i kombination med andra väl etablerade källor inom området. Den täcker alla de områden som säkerhetsarbetet behöver omfatta, ledning, organisation och ansvarsfördelning, det rent tekniska skyddet och det som handlar om att påverka de anställdas beteende.

Vad kan bristande informationssäkerhet leda till?

Socialförsäkringsadministrationen, dvs. Riksförsäkringsverket och försäkringskassorna (vilket i dag motsvarar Försäkringskassans verksamhet) hade 2004 en verksamhetsomsättning om 8,5 miljarder kronor och administrerade utgifter i socialförsäkringen som sammantaget uppgick till 426 miljarder kronor. Detta motsvarade omkring hälften av det av riksdagen fastställda utgiftstaket. Av 100 kr som

används för privat konsumtion kommer 25 från socialförsäkringen[1]. Varje dag sker utbetalningar till ett mycket stort antal människor. Det utbetalade beloppet per dag är ca 1,5 miljarder kronor från socialförsäkringssystemen. Utbetalningarna sker genom betalningsuppdrag till bankerna.

Av regeringens regleringsbrev till Försäkringskassan för verksamhetsåret 2005 framgår att riskerna för störningar ska minimeras och samhällets grundläggande behov av ekonomisk säkerhet ska tillgodoses vid svåra påfrestningar på samhället i fred. Störningar i Försäkringskassans förmåga att leverera riktiga betalningar påverkar försörjningen hos en stor del av befolkningen.

En stor del av den information som hanteras av Försäkringskassan är personuppgifter. Brister i förmågan att skydda personuppgifter kan dels leda till skada för enskild, dels äventyra allmänhetens förtroende för Försäkringskassan.

Har Försäkringskassan ett väl fungerande ledningssystem för informationssäkerhet?

De delar av ledningssystemet för informationssäkerhet som utgörs av ansvarsfördelning, tekniska skyddsåtgärder och styrdokument finns till största delen på plats.

Granskningen visar att ledningens informationssäkerhetsarbete har tre huvudsakliga brister: överblicken, riskanalysen och uppföljningen. Dessa brister påverkar i sin tur ledningens förmåga att uppnå och vidmakthålla eftersträvad informationssäkerhet.

Svaret på den fråga som granskningen syftat till att besvara är därmed att Försäkringskassan inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

De delar som Försäkringskassan framför allt bör utveckla är följande:

- *Förmågan till överblick över informationstillgångarna, riskerna samt säkerhetsåtgärderna (införda, beslutade och planerade).*
  Verksledning och verksamhetschefer på huvudkontoret saknar enligt vår bedömning tillräckligt stöd och hjälpmedel för att skapa en rättvisande och överblickbar bild över informationssäkerhetsriskerna i verksamhetens skilda delar – centralt, lokalt och inom IT-verksamheten[2]. Denna brist på möjligheter att överblicka

[1] Källa: Socialförsäkringens årsredovisning för budgetåret 2004.

[2] Bl.a. enskilda försäkringsslag/produkter, utifrån geografisk belägenhet, med avseende på typ av risk, m.fl. aspekter.

riskerna medför enligt Riksrevisionens bedömning bl.a. svårigheter för myndighetsledningen att avgöra om beslutade säkerhetsåtgärder inom skilda verksamheter är i linje med av riksdag och regering beslutade normer eller av verksledningen fattade beslut.

- *Styrningen av arbetet med riskanalyser för att säkerställa att de väsentliga riskerna beaktas.*
  En brist är avsaknad av organisering och styrning av samlade analyser av informations- och IT-säkerhetsrisker för Försäkringskassan som helhet. Ingen har getts ett tydligt utpekat ansvar för att göra eller sammanställa en samlad riskanalys beträffande informationssäkerhet för Försäkringskassan. Med samlad riskanalys menas här en från verksamheterna underbyggd riskanalys. Riskanalys är inte en väl integrerad del i systemutvecklingen, vilket kan leda till att säkerhetsrisker beaktas sent i utvecklingsprojekten eller i efterhand när systemen är driftsatta, vilket kan medföra dyrbara kompletterande säkerhetsåtgärder eller att risker inte uppmärksammas alls förrän incidenter inträffar.
- *Ledningens uppföljning av hur ledningssystemet för informationssäkerhet fungerar samt uppföljning av säkerhetsåtgärder.*
  På en övergripande nivå saknar Försäkringskassan en sammanhållen åtgärdslista för säkerhetsåtgärder och uppföljning av dessa åtgärder. Försäkringskassan kan därför inte ge en samlad bild av hur de befintliga säkerhetsåtgärderna, och uppföljningen av dessa, tillsammans ger ett fullgott skydd.

1 Inledning

1.1 Bakgrund, syfte och revisionsfrågor

1.1.1 Bakgrund

Granskningen avser Försäkringskassans informationssäkerhet. Informationssäkerhet omfattar

- konfidentialitet/sekretess, dvs. att endast behöriga användare kommer åt informationen i verksamhetens informationssystem,
- tillgänglighet, dvs. att behöriga användare har tillgång till den information och de funktioner de är behöriga till i rätt tid och omfattning för att kunna ge en god service,
- riktighet (informations/datakvalitet), dvs. att information inte obehörigt ändras eller modifieras,
- spårbarhet, dvs. att kunna se vem som gjort vad och vid vilken tidpunkt, t.ex. om informationen påverkats i strid med myndighetens regler.

Informationssäkerheten är väsentlig därför att elektronisk förvaltning får insteg hos de flesta statliga myndigheter och allt större krav ställs på att sådana tjänster är säkra, inte minst för att medborgare och företagare ska ha förtroende för dessa tjänster. Med denna utveckling följer bl.a. att myndigheterna löpande behöver se över och vid behov förstärka skyddet mot de risker som följer bl.a. av den elektroniska förvaltningen.

En rapport[3] från Sveriges IT-incidentcentrum, Sitic, som är en del av Post- och telestyrelsen, visar följande:

- 21% av offentliga[4] organisationer har någon gång varit med om IT-säkerhetsincidenter som medfört att information eller systemkomponenter blivit åtkomlig för obehörig att läsa, kopiera, ändra eller radera. Det kan alltså handla om dataintrång, hacking.
- 10% av offentliga organisationer har varit med om IT-säkerhetsincidenter som inneburit en utförlig kartläggning av deras system. Det handlar alltså om att obehörig letat efter sårbara punkter på ett sätt som skiljer sig från det vardagliga mönstret.

---

[3] Uppgifterna är ett resultat av en bearbetning som, enligt önskemål från Riksrevisionen, Sitic gjort av sin mörkertalsundersökning, http://www.pts.se/Archive/Documents/SE/Morkertalsundersokningen_2005.pdf.

[4] Det vill säga statliga och kommunala myndigheter.

- 20% av offentliga organisationer har varit med om IT-säkerhetsincidenter som medfört att system eller delar av system blev otillgängliga, s.k. DOS-angrepp eller Denial of Service. Det kan alltså handla om att system eller nätverk blivit överbelastat på grund av ett DOS-angrepp.
- 30% av offentliga organisationer har varit med om IT-säkerhetsincidenter som inneburit ett allvarligt utbrott av skadlig kod med betydande konsekvenser för verksamheten. Det kan alltså handla om så kallade virus, ”maskar”, ”trojaner” m.m.

Sitics undersökning visar att både hot och incidenter är verklighet för svenska myndigheter i dag.

1.1.2 Syfte

Granskningen avser Försäkringskassans arbete med informationssäkerhet. Under arbetets gång har Riksrevisionen valt att fokusera på ledningen av arbetet med informationssäkerhet. Vi har vidare valt att avgränsa granskningen till arbete med säkerheten för de IT-relaterade informationstillgångana. Därmed har vi inte granskat säkerheten för manuella register, brev och liknande informationssamlingar[5]. Anledningen till vårt val är att skyddet av de IT-relaterade informationstillgångarna är den mest svårbemästrade delen av informationssäkerheten eftersom den förutsätter en väl strukturerad och fungerande samverkan mellan individer och många gånger mycket komplicerade tekniska system. Det är också så att det främst är denna del av myndighetens informationshantering som har att motstå en mängd nya hot.

I granskningen har tyngdpunkten således legat på myndighetsledningens styrning och kontroll för att säkerställa säkerheten hos eller skyddet av informationen i IT-systemen och andra informationstillgångar, såsom systemdokumentation, programkod och programlicenser. Denna styrning och kontroll benämns samlat myndighetens ledningssystem för informationssäkerhet (LIS). Denna avgränsning innebär bl.a. att faktiskt uppnådd säkerhet i enskilda system inte granskats[6]. God informationssäkerhet uppstår inte av en händelse utan kräver ett systematiskt säkerhetsarbete som leds utifrån noggranna analyser av bl.a. verksamhetens säkerhetsbehov, sårbarhet och risker. LIS är alltså en viktig förutsättning för god informationssäkerhet.

Betydelsen av LIS som förutsättning för god informationssäkerhet är särskilt stor i omfattande och komplexa verksamheter med stora och svåröverblickbara IT-system. Detta är bakgrunden till vårt val av LIS som fokus.

---

[5] Riksrevisionen är dock medveten om att det hos Försäkringskassan finns stora mängder ärendeakter med pappersbunden information.

[6] Däremot har Riksrevisionen tagit del av rapporter som avser skyddet i vissa enskilda system.

Revisionsfrågan är: Arbetar myndigheterna, utifrån gängse normer, systematiskt med sin informationssäkerhet?

1.2 Bedömningskriterier

Riksrevisionen har utgått från ett flertal normkällor[7]. Standarden Ledningssystem för informationssäkerhet – Riktlinjer för ledning av informationssäkerhet (SS-ISO/IEC 17799 och SS 627799) är grunden för Riksrevisionens granskningskriterier. LIS-standarden utgör riktlinjer som enligt standarden "bör betraktas som ett underlag för att utveckla organisationsspecifika riktlinjer. Allt som nämns i denna standard är kanske inte tillämpligt. Ytterligare åtgärder, som inte anges i denna standard, kan också vara nödvändiga."[8] Samtidigt utgör standarden "en gemensam grund för i princip alla organisationer."[9]

För Riksrevisionens beslut har följande faktorer haft betydelse:

- LIS-standarden är den mest fullständiga normkällan. Den täcker alla de områden – länkarna i kedjan – som säkerhetsarbetet behöver omfatta för att eftersträvad säkerhet ska kunna uppnås.
- Den är den enda internationella standarden för informationssäkerhet som täcker hela detta område.
- Stora delar av både näringsliv och förvaltning har accepterat den som utgångspunkt för det egna arbetet med informationssäkerhet.
- Standardens innehåll (riktlinjerna) har visats sig vara stabilt. Standarden har efter 10 år nu uppdaterats beträffande sin disposition men den är innehållsligt intakt.

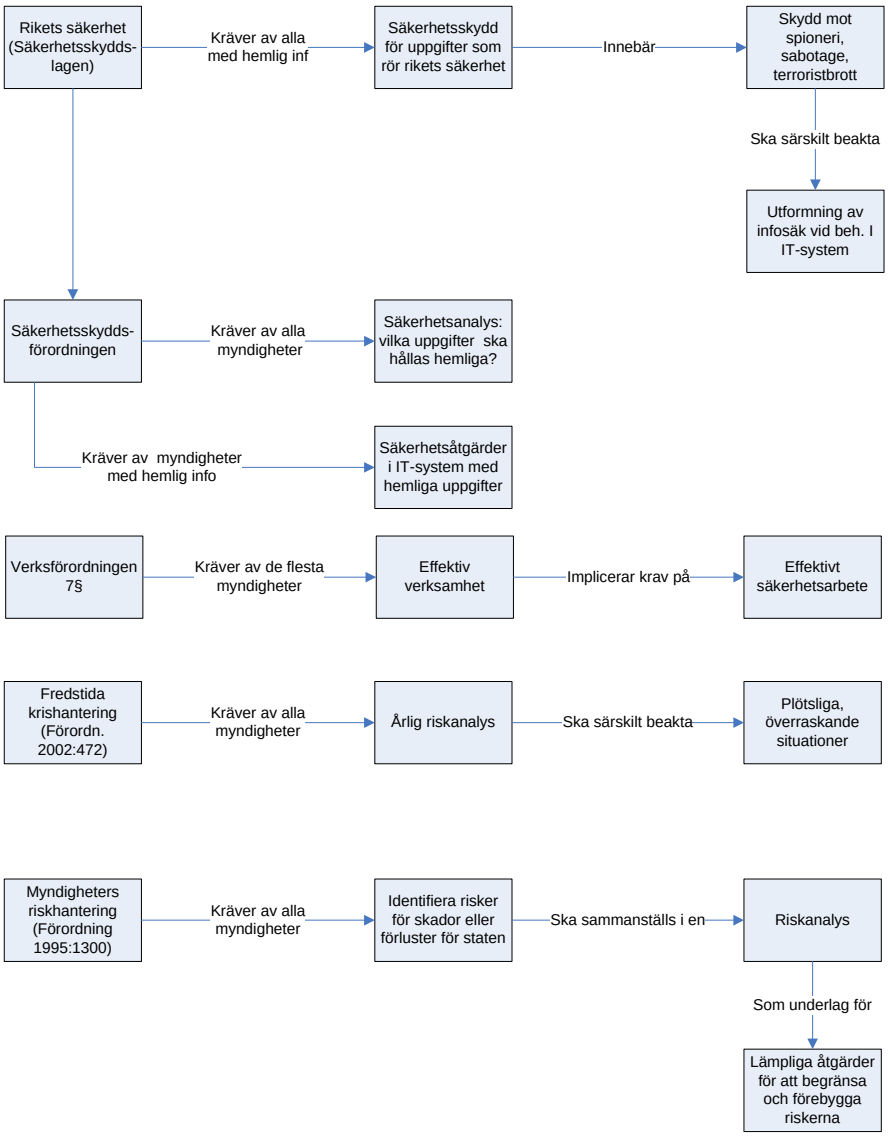
---

[7] Standarden Ledningssystem för informationssäkerhet, Krisberedskapsmyndighetens rekommendation BITS, Basnivå för IT-säkerhet, Verksförordningen (1995:1322), Förordning om myndigheters riskhantering (1995:1300), Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, Säkerhetsskyddsförordning (1996:633, 2000:888), Datainspektionens föreskrifter om bearbetning av personuppgifter i datorer, "800-serien" från USA:s standardiseringsorgan NIST, COBIT, *Control Objectives for Information and related Technology,* erfarenheter från andra nationella revisionsorgan, bl.a. GAO i USA, OAG i Kanada, samt erfarenheter från den svenska bank- och försäkringssektorn.

[8] SS-ISO/IEC 17799 sidan 10.

[9] SS-ISO/IEC 17799 sidan 10.

1.2.1 *Översikt av lagar och förordningar som berör informationssäkerhet*



Figur 1. Översikt över reglering av informationssäkerhet.

Lagar och förordningar som berör informationssäkerhetsområdet beskrivs i figuren ovan[10]. De behandlar myndigheters riskhantering (förordning [1995:1300] om myndigheters riskhantering), åtgärder för fredstida krishantering (förordning [2002:472] om åtgärder för fredstida krishantering och höjd beredskap), skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet (säkerhetsskyddslagen [1996:627]).

[10] Redovisningen utgör ett urval som bedömts relevant. Därutöver finns bl.a. RPS föreskrifter (RPS FS 1996:9), skyddslagen (1990:217) och sekretesslagen (1980:100).

Vad som berör **samtliga myndigheter** är

- kravet att utföra en *riskanalys* som identifierar risker för skador och förluster för staten (3 § förordning om myndigheters riskhantering)
- kravet att vidta *lämpliga åtgärder* för att begränsa riskerna och förebygga skador eller förluster (3 § förordning om myndigheters riskhantering)
- kravet att utföra årlig *risk- och sårbarhetsanalys* som ska identifiera sårbarhet och risker som synnerligen allvarligt kan påverka verksamheten. Särskilt ska beaktas situationer som uppstår hastigt, oväntat och utan förvarning, sådana som allvarligt påverkar samhällets funktionsförmåga samt myndighetens förmåga att hantera mycket allvarliga situationer inom ansvarsområdet (3 § förordning om åtgärder för fredstida krishantering och höjd beredskap).
- kravet att utföra *säkerhetsanalys* som ska visa om myndigheten har information som ska hållas hemlig med hänsyn till rikets säkerhet (5 § säkerhetsskydds-förordning).

Vad som berör **vissa myndigheter**, de som enligt genomförd säkerhetsanalys har information som med hänsyn till *rikets säkerhet* ska hållas hemlig, är

- krav att det ska finnas det *säkerhetsskydd* som behövs som skydd mot spioneri, terroristbrott m.m. som kan hota rikets säkerhet (5 § säkerhetsskyddslagen) och som förebygger brister i informationssäkerhet som avser hemlig information (7 och 9 §§ säkerhetsskyddslagen)
- krav på *särskilda säkerhetsåtgärder* – behörighetskontrollsystem, händelseloggning, samråd med säkerhetsmyndigheterna i vissa fall, godkänd kryptering, inventering av hemliga handlingar – för de IT-system som används för hemlig information (12 §, säkerhetsskyddsförordningen). Regeringen har här alltså funnit anledning att formulera relativt konkreta krav på dessa myndigheters säkerhetsarbete till den del detta avser skydd av hemlig information.

Risker för skador och förluster för staten kan skapas av brister i informationssäkerheten för stora delar av den statliga informationen och inte bara i den hemliga informationen. Riskhanteringsförordningen innehåller därmed implicit ett krav på riskanalys också beträffande informationssäkerhet. Vidare krävs att lämpliga skyddsåtgärder vidtas för att begränsa och förebygga riskerna. Riksrevisionen uppfattar därför Riskhanteringsförordningen som den mest långtgående i kraven på alla myndigheters informationssäkerhetsarbete. Samtidigt avgränsas riskerna till sådana som har statsfinansiell betydelse. Risker för enskildas intressen lämnas därmed utanför om de inte föranleder ersättningsanspråk på staten.

Regeringen vill vidare att myndigheterna i risk- och sårbarhetsanalysen lyfter upp riskerna för att hemlig information röjs eller förvanskas och på så sätt allvarligt påverkar samhällets funktionsförmåga eller förmågan att hantera mycket allvarliga situationer (3 § krishanteringsförordningen).

Enligt Riksrevisionens tolkning av LIS-standarden ska all, enligt den enskilda myndighetens bedömning, *skyddsvärd information* skyddas. Det innebär ett vidgat åtagande eftersom skyddsvärdet inte relateras till enbart rikets säkerhet eller till statsfinansiella förluster utan kan avse exempelvis enskilds integritet och hälsa eller hemliga förhållanden i företag. Det som enligt regelverket ska göras av alla myndigheter – riskanalys, risk- och sårbarhetsanalys samt säkerhetsanalys – inryms samtidigt i standardens krav på främst ledningssystemets riskanalysprocess respektive den del av riskanalysen som avser säkerhetsklassning av informationen.

Riksrevisionens slutsats är att ingenting i LIS-standarden motsäger regelverket. Skillnaderna är att regelverket täcker en mindre del av myndigheternas säkerhetsarbete (främst riskanalysen) och en mindre del av de statliga informationstillgångarna samt att regelverket är mindre preciserat med undantag för säkerhetsarbetet som gäller den hemliga informationen. LIS-standarden kan på så sätt sägas precisera kraven på myndigheternas arbete inom informationssäkerhetsområdet. Det ska tilläggas att det enligt Riksrevisionens bedömning även följer av verksförordningens 7 § – att myndighetens verksamhet ska bedrivas effektivt – att myndigheter ska bedriva ett effektivt säkerhetsarbete. Detta krav torde enligt Riksrevisionens bedömning innebära bl.a. att säkerheten för alla skyddsvärda informationstillgångar ska skötas i ett sammanhållet ledningssystem. Då skapas också möjligheterna för myndighetsledningen att i realiteten ta ett samlat ansvar för informationssäkerheten. LIS-standarden innehåller de mest väsentliga kraven på ett sådant ledningssystem.

Riksrevisionen har därför tagit fram ett granskningsprogram med kriterier och intervjufrågor som avser LIS och som baseras på LIS-standarden. Frågorna har strukturerats efter den interna styrningen och kontrollens olika beståndsdelar enligt den s.k. COSO-modellen.

Granskningsprogrammet har behandlats i seminarier med Swedish Standards Institute (Sis), Krisberedskapsmyndigheten, Statskontoret och en säkerhetschef inom bank- och försäkringssektorn.

1.3 Metoder och tillvägagångssätt i granskningen

Granskningen har genomförts på följande sätt:

- Myndigheten har först fått ett introduktionsbrev och en begäran att förse Riksrevisionen med styrdokument inom området, bl.a. informationssäkerhetspolicy.
- Myndigheten har därefter fått besvara ett frågeformulär (dvs. en självutvärdering) om myndighetens syn på sin verksamhet och behovet av informationssäkerhet. Myndigheten redovisar vidare vilka delar av det ledningssystem för informationssäkerhet som standarden anger som finns i myndighetens ledningssystem för informationssäkerhet.
- Myndigheten har i nästa steg fått en lista som beskriver s.k. nyckeldokument som Riksrevisionen behöver för sin granskning. Myndigheten har sedan översänt dessa. Myndigheten har gjort en egen bedömning vilka av dess dokument som motsvarar Riksrevisionens beskrivningar och som tillsammans ger en rättvisande bild av myndighetens ledningssystem för informationssäkerhet.
- Efter det att Riksrevisionen gått igenom dokumenten har företrädare för myndigheten blivit intervjuade[11] med stöd av granskningsprogrammets intervjufrågor. Eftersom Försäkringskassan har en stor regional och lokal organisation, har intervjuer även genomförts vid två länskontor. Intervjuerna spelades in – efter att intervjupersonerna lämnat sitt medgivande – för att öka precisionen i tolkningarna av intervjuerna. Efter intervjuerna har en del kompletterande dokument överlämnats till revisionen.
- Riksrevisionen har därefter, på Försäkringskassan önskemål, muntligen redovisat den problembild som vuxit fram. Försäkringskassan har därefter överlämnat ytterligare kompletterande information.
- Myndigheten har sedan faktagranskat utkastet till revisionsrapport.

1.4 Läsanvisningar

Begreppet ”systematisk” används på flera ställen. Det står för ett förfarande som till sin natur är metodiskt och av ledningen fastställt.

Ett annat ord som används är ”tillräcklig”. Det är en bedömning som Riksrevisionen gör av hur långt vi bedömer att Försäkringskassan kommit i förhållande till vår tolkning[12] av de krav som uttrycks i LIS-standarden.

---

[11] GD, ÖD, cheferna för utvecklingsdivisionen respektive produktionsdivisionen, säkerhetschefen, informationssäkerhetschefen, IT-säkerhetschefen, länsdirektör och lokal säkerhetssamordnare.

[12] Exempel: Om beskrivningen av myndighetens informationsresurser är spridd på ett flertal dokument eller databaser gör vi bedömningen att den samlade beskrivningen som dessa dokument utgör inte är tillräckligt överblickbar och därmed inte direkt användbar för säkerhetsklassningsarbetet.

I rapporten har redovisningen av granskningskriterier, iakttagelser och slutsatser strukturerats[13] enligt följande:

- kontrollmiljö
- riskanalys
- kontrollfunktioner och säkerhetsåtgärder
- information och utbildning
- uppföljning och utvärdering

En beskrivning av Riksrevisionens bedömningskriterier för respektive komponent i modellen inleder kapitlen 3–7. Dessa kapitel behandlar Riksrevisionens iakttagelser och slutsatser.

Alla bedömningskriterier identifieras med fetstilta ledord i kapitlens inledande avsnitt om bedömningskriterier. I de därpå följande avsnitten om iakttagelser används dessa fetstilta ledord för att underlätta för läsaren. I vissa kapitel saknas iakttagelser beträffande en del av dessa kriterier. Riksrevisionen har under granskningens gång fokuserat vissa kriterier och tillhörande frågor med ledning av de uppgifter som framkommit. Dessa kriterier skrivs fetstilt i respektive kapitels avsnitt för iakttagelser. Även de bedömningskriterier som inte motsvarats av iakttagelser har dock tagits med eftersom Riksrevisionen bedömt det vara av värde att redovisa även övriga kriterier. En mer fullständig redovisning kan t.ex. vara av värde för Försäkringskassan i en sådan genomgång av myndighetens informationssäkerhetsarbete som Riksrevisionens rekommendationer innebär. Att ett kriterium inte tagits upp bland iakttagelserna innebär alltså inte att Riksrevisionen funnit att detta uppfylls av myndigheten. Bedömningarna som följer sist i varje kapitel tar endast upp de iakttagelser som utgör den huvudsakliga grunden för Riksrevisionens slutsatser

[13] Committee of Sponsoring Organizations of the Treadway Commission (COSO) har beskrivit den interna styrningens och kontrollens olika beståndsdelar och deras samband i den s.k. COSO-modellen. Strukturen för denna rapport motsvarar dessa beståndsdelar.

2 Försäkringskassan och informationssäkerheten

2.1 Försäkringskassans verksamhet m.m.

Den 1 januari 2005 inrättades Försäkringskassan. Den nya myndigheten ersatte Riksförsäkringsverket och de 21 allmänna försäkringskassorna. Försäkringskassan[14] administrerar de försäkringar och bidrag som ingår i socialförsäkringen. Myndigheten har c:a 16 000 medarbetare. I varje län finns ett länskontor och flera försäkringskontor. Totalt finns c:a 240 försäkringskontor. Huvudkontoret ligger i Stockholm.

År 2004 var socialförsäkringens utgifter sammanlagt 426 miljarder kronor. Dagligen utbetalas ca 1,5 miljarder kronor från socialförsäkringssystemen, vilket sker genom betalningsuppdrag till bankerna. Utbetalningarna från socialförsäkringen är en betydande del av samhällsekonomin.

Socialförsäkringarna finansieras främst genom socialavgifter från arbetsgivare och egenföretagare, allmän pensionsavgift, statliga ålderspensionsavgifter, statliga medel samt fondavkastning. Vissa försäkringsförmåner finansieras helt med statliga medel.

Föreskrifter, allmänna råd och vägledningar som beslutats av Riksförsäkringsverket gäller även efter Försäkringskassans inrättande.

De förvaltningsrättsliga föreskrifter som reglerar Försäkringskassans verksamhet är förutom regleringsbrevet och instruktionen

- förvaltningslag (1986:223)
- förvaltningsprocesslag (1971:291)
- tryckfrihetsförordning (1949:105) (omtryck 2002:908)
- sekretesslag (1980:100)
- lag (2004:115) om självbetjäningstjänster via Internet inom socialförsäkringens administration
- personuppgiftslag (1998:204)
- lag (2003:763) om behandling av personuppgifter inom socialförsäkringens administration
- lag (1992:1528) om offentlig upphandling
- lag (1962:382) angående införande av lagen om allmän försäkring.

[14] I stora stycken hämtat från Försäkringskassans webbplats.

Därutöver finns en stor mängd föreskrifter som Försäkringskassan utfärdat och som reglerar handläggningen av försäkringsärendena.

2.2 Informationstillgångarna och Försäkringskassans bedömning av säkerheten för dessa

Inslaget av IT-stöd i Försäkringskassans processer är betydande, och Försäkringskassan är starkt IT-beroende. Försäkringskassans IT-stöd är ett av statsförvaltningens mest omfattande.

Det ställs stora krav på att den information som finns i Försäkringskassans informationssystem är säkerställd. Med detta menas att informationens riktighet, tillgänglighet, sekretess samt spårbarhet är skyddad.

Enligt Riksrevisionens enkät till myndigheten betraktar Försäkringskassan informationssäkerhet som en viktig ledningsfråga, vilket också bekräftas av de personer vi intervjuat.

Flera faktorer i myndighetens verksamhet påverkar Försäkringskassans bedömning av informationssäkerhetens betydelse i verksamheten. Försäkringskassan framhåller i sitt svar på Riksrevisionens webbenkät att volymen förvaltade anläggningstillgångar, storleken hos penningströmmarna, omfattningen av IT-beroendet, volymen integritetskänslig information, volymen sekretesskänslig information, volymen ärenden som behandlas och vikten av kontinuitet i verksamheten är särskilt betydelsefulla faktorer för utformningen av arbetet med informations- och IT-säkerhet.

Sammantaget anser Försäkringskassan enligt enkätsvaret att myndigheten har en informationssäkerhet som är behäftad med vissa mindre brister.

2.2.1 Viktiga IT-system hos Försäkringskassan

Försäkringskassans IT-system finns i huvudsak i Sundsvall där driften sker.

För att ge läsaren en bild av vilka viktiga IT-system och förmåner som hanteras i IT-system som finns hos Försäkringskassan anges här några av de viktigaste:

Ålderspension och Förtidspension

Pensionsutbetalningarna inom områdena Ålderspension och Förtidspension ska ge pensionstagarna rätt pension då de lämnar arbetslivet på grund av ålder eller ohälsa. De som har låg inkomstpension eller ingen alls har rätt till Garantipension.

Sjukpenning, Föräldrapenning och Utbildningsbidrag

Dagersättning inom områdena Sjukpenning, Föräldrapenning och Utbildningsbidrag utgör ersättning för förlorad arbetsinkomst på grund av sjukdom, barnafödande eller utbildning.

Assistansersättning

Assistansersättning (LASS) är en förmån för personer som har svåra funktionshinder och behöver ett personligt utformat stöd för att klara vardagen. Personlig assistans med de grundläggande behoven innebär bl.a. hjälp med personlig hygien, att klä på och av sig, att äta och att meddela sig med andra personer.

Barnbidrag och Underhållsstöd

Barnbidrag är en av flera familjeförmåner som syftar till minska de ekonomiska skillnaderna mellan hushåll med och hushåll utan barn.

Underhållsstöd är en förmån där samhället garanterar att barn får pengar till sin försörjning från den förälder som barnet inte bor tillsammans med.

Bostadsbidrag till barnfamiljer

Förmånen ska ge ekonomiskt svaga hushåll en möjlighet att hålla sig med goda och tillräckligt rymliga bostäder. Därutöver ska förmånen bidra till att minska de ekonomiska skillnaderna mellan hushåll med barn och hushåll utan barn.

Bostadsstöd för pensionärer

Bostadstillägg till pensionärer är en förmån som ersätter en del av kostnaderna för boendet.

Ärendehanteringssystemet

Ärendehanteringssystemet (ÄHS) är ett system som används inom flera förmånsslag bl.a. för att besluta i ärenden.

Generell personinformation

Generell personinformation (GPI) är ett försystem som används för alla förmåner. I detta system lagras och distribueras all personrelaterad information om alla försäkrade som efterfrågas av försäkringssystemen.

Store

Store är Försäkringskassans datalager och där finns information om hela Sveriges befolkning inom socialförsäkringsområdet.

Utbred och Netto

Utbred och Netto är Försäkringskassans utbetalnings- och redovisningssystem som utnyttjas för samtliga förmåner. Utbred ligger i gammal datormiljö och Netto i ny datormiljö.

3 Kontrollmiljön

3.1 Bedömningskriterier

Kontrollmiljön är en del av myndighetskulturen och skapas av myndighetens ledning och chefer i interaktion med medarbetarna och omgivningen.

Verksledningen bör skapa tillräckliga **förutsättningar** för arbetet med informationssäkerheten. Viktiga förutsättningar är lämpliga organisatoriska former för arbetet med informationssäkerhet, uttalat stöd till dem som arbetar med informationssäkerhet samt resurser som står i paritet med ledningens krav på skyddet av informationstillgångarna.

Verksledningen i statliga myndigheter bör noga avväga[15] det **engagemang** som ska ägnas informationssäkerhetsfrågorna vid sidan av övriga ledningsuppgifter. Av särskild vikt är det att detta görs i sådana myndigheter som har informationstillgångar som är av avgörande betydelse för verksamheten, är sekretessbelagda eller har stora databaser som avser enskilda eller företag och som därmed kan vara känsliga om de sprids. Detta engagemang och tillhörande syn på betydelsen av intern styrning och kontroll av informationssäkerhetsarbetet bör också kommuniceras till medarbetarna.

Att verksledningen lägger vikt vid informationssäkerheten bör också framgå av att den skaffat sig tillräcklig **förtrogenhet** med de ledningsfrågor som informationssäkerhetsarbetet innehåller.

Verksledningen bör tillse att de krav och mål som ska gälla för informationssäkerheten tydligt förmedlas till alla berörda IT-användare inom myndigheten. Detta bör göras i ett sammanhållet övergripande policydokument, en **informationssäkerhetspolicy**. Medarbetarna bör delges vikten av att informationssäkerhetskraven och övriga krav i informationssäkerhetspolicyn uppfylls samt vilka konsekvenser som i annat fall uppstår för den enskilde medarbetaren.

3.2 Iakttagelser

Försäkringskassans val av organisation för arbete med informationssäkerhet grundas till stor del på slutrapporten från projektet Administration som

[15] Ledningen bör kunna beskriva sina överväganden på ett konsistent sätt.

ingick i GEORG[16]. Förslagen, som rör informationssäkerheten, är främst följande:

- En övergripande organisationsstruktur för säkerhetsorganisationen ska införas i den nya myndigheten. Strukturen omfattar säkerhetschef placerad i stab i ledningens närhet, informationssäkerhetsenhet (för all information oavsett informationsbärare) vid Produktionsdivisionen, IT-säkerhet med IT-säkerhetschef vid IT-avdelningen, samverkan mellan säkerhetsfunktionerna, säkerhetssamordnare på länsnivå för alla säkerhetsområden, säkerhetssamordnare vid systemägarorganisationer och utvecklingsdivisionen, lokala säkerhetsombud vid varje ort/kontor, vissa samverkansformer för säkerhet samt delegering av beslutsrätt inom säkerhetsområdet.
- Säkerhetschefens och informationssäkerhetschefens ansvar och befogenheter tydliggörs.
- Det är ledningens ansvar att se till att det finns en väl fungerande organisation för säkerhetsarbetet. Den som är ansvarig för någon del av verksamheten har också ansvaret för säkerheten (utbildning, information, att utse befattningshavare, uppföljning och kontroll av skyddsnivå, efterlevnad av regler). Resurser måste finnas i organisationen för att normera och samordna säkerhetsarbetet samt stödja linjeansvariga.

Försäkringskassan har utarbetat ett antal styrdokument för att styra arbetet med informationssäkerhet, vilka sammantaget motsvarar innehållet i en **informationssäkerhetspolicy.** I styrdokumentet Riktlinjer för informationssäkerhet definieras området, viktiga begrepp förklaras, grunden för vald LIS framgår, en beskrivning ges av 16 delområden, bl.a. mål för säkerhetsarbetet, ansvar och regler, informationssäkerhetsprocessen, riskhantering, olika typer av säkerhetsåtgärder och kontrollfunktioner, information och utbildning samt uppföljning och kontroller.

Några av de mer centrala dokumenten i detta sammanhang ur ledningens perspektiv är arbetsordning, säkerhetspolicy för Försäkringskassan, riktlinjer för allmän säkerhet, riktlinjer för krisberedskap, riktlinjer för informationssäkerhet samt beslut om Försäkringskassans säkerhetsorganisation. I dessa styrdokument regleras under vilka **förutsättningar** arbetet med informationssäkerhet ska bedrivas i form av organisation och ansvar, vilka regler som gäller samt hur styrning och uppföljning ska gå till.

Enligt säkerhetspolicyn har generaldirektören det övergripande ansvaret[17] för säkerheten inom Försäkringskassan. Av säkerhetspolicyn framgår vidare att verksamhetsansvarig chef ansvarar för säkerheten inom

[16] Försäkringskassans genomförandeorganisation GEORG, SOU 2004:127.

[17] Detta ansvar har GD i första hand inför styrelsen som enligt instruktionen har ansvaret för verksamheten.

sin verksamhet; säkerhetsansvaret följer således ”linjeansvaret”. I detta ansvar ingår att i den årliga verksamhetsplaneringen ta fram handlingsplaner för säkerhet.

För att stödja verksamhetsansvarig i säkerhetsarbetet finns följande säkerhetsfunktioner och -roller beskrivna:

- Säkerhetschef, informationssäkerhetschef med en informationssäkerhetsenhet samt IT-säkerhetschef med en IT-säkerhetsgrupp[18].
- Säkerhetssamordnare som utses av divisionschefer och länsdirektörer att verka inom divisionen/länet.
- Lokala säkerhetsombud som utses av verksamhetsansvariga chefer på respektive lokaliseringsort.
- Samverkansformer såsom återkommande möten mellan säkerhetsfunktionerna, säkerhetsråd och incidentråd.

Den verksamhetsansvarige på respektive nivå ansvarar för att säkerheten inom den delen av verksamheten fungerar; till stöd för detta finns ett antal funktioner av specialistkaraktär som har till ansvar att stödja de verksamhetsansvariga i säkerhetsfrågorna. Flera intervjuade anser dock att säkerhetspersonalen agerar utan tydlig och systematisk styrning eller uppföljning från verksamhetsansvariga.

Det framgår också av styrdokumenten att det är vars och ens ansvar att ta del av anvisningar och regler för säkerhet. Personalen ska kunna säkerhetsfrågorna. All personal ska vara medveten om hot och risker som rör informationssäkerheten.

Av säkerhetspolicyn framgår att Försäkringskassan ska bedriva sitt arbete med informationssäkerhet i enlighet med standarden ISO 17799. Detta innebär bl.a. innebär att ett ledningssystem för informationssäkerhet ska finnas vid myndigheten.

Av arbetsordningen framgår att säkerhetschefen har det övergripande ansvaret för samordning av säkerhetsarbetets skilda domäner (personsäkerhet, informationssäkerhet m.fl.) inom myndigheten, samt att besluta om riktlinjer och rutiner för säkerhet.

LIS-standarden anger att ett uttryck för ledningens **engagemang** för informationssäkerhet är att ledningen preciserar ett ansvar och aktiviteter för att få nödvändig överblick av informationstillgångarna så att det blir möjligt att göra en riktig prioritering av skydd och skyddsåtgärder. Prioriteringen ska enligt standarden baseras på en riskanalys. För Försäkringskassans del finner vi att detta ansvar inte är tillräckligt tydligt utpekat i styrdokumenten.

[18] Försäkringskassan tog den 27 januari 2006 beslut om ny säkerhetsorganisation för informationssäkerheten. Detta beslut har inte beaktats i granskningen.

Detta leder både till otydlighet i riskanalysen och till att ledningens förmåga till överblick försvagas. Vi återkommer till detta i kapitel 4 om riskanalysen.

Ingen har i styrdokumenten ett tydligt utpekat ansvar för att göra eller sammanställa en samlad, övergripande riskanalys för hela Försäkringskassan. Vi finner inte heller någon sådan analys. Till detta återkommer vi i kapitel 4.

Ledningens uppföljning är en annan viktig del av engagemanget för informationssäkerheten. På vilket sätt ledningen ska följa upp det delegerade ansvaret för informationssäkerheten har dock inte tydliggjorts i styrdokumenten. Ledningens uppföljning bygger på incidentrapportering och incidenthantering, dvs. hantering av uppkomna brister i verksamhetens säkerhet. Vi saknar alltså en systematisk uppföljning utöver detta, dvs. att de säkerhetsåtgärder som prioriterats och beslutats av ledningen fullföljs i enlighet med en beslutad åtgärdsplan. En effekt av detta kan möjligen vara en brist som lyfts fram av flera intervjuade, nämligen att frågor rörande informationssäkerhet vid verksamhetsutveckling inte beaktas i tillräcklig utsträckning, trots att detta upplevs som prioriterat av ledningen. En annan dimension av säkerhetsarbetet är den geografiska spridning som Försäkringskassan har. Det lokala säkerhetsarbetet i länsorganisationen styrs av de centrala styrdokumenten. Utöver det förekommer samarbete framför allt i säkerhetsråd, säkerhetskonferens och myndighetsgemensamma säkerhetsprojekt. Det finns dock ingen samordnad verksamhetsplanering eller input till gemensamma planeringsfrågor för säkerhetsarbetet i länsorganisationen, inte heller någon ensad eller samlad uppföljningsansats från huvudkontoret, t.ex. inför kommande verksamhetsplanering. Detta kan leda till olika prioriteringar i de olika länsorganisationerna.

Beträffande ledningens **förtrogenhet** med informationssäkerhetsarbetets ledningsfrågor kan konstateras att ledningsgruppen inte genomgått någon särskild utbildning när det gäller detta. Försäkringskassan har dock under året bedrivit en utbildning som riktats mot samtliga anställda (se även kapitel 6).

3.3 Bedömning

De ovan beskrivna bristerna vad gäller övergripande riskanalys och förmåga till översikt medför risk att riskanalysen och prioriteringen av införande av kontrollåtgärder inte bygger på en tillräckligt god grund för att ge en god informationssäkerhet.

Det finns oklarheter i den organisatoriska lösningen för arbetet med informationssäkerhet. Ingen har ett tydligt uttalat ansvar för den övergripande riskanalysen. Styrning och samverkan mellan det centrala och det lokala

säkerhetsarbetet är inte heller fullt utvecklade, vilket bl.a. kan leda till brister i enhetlighet i synen på vilka skyddsåtgärder som ska prioriteras och genomföras.

Krav på informationssäkerhet behandlas inte som funktionalitetskrav vid system- och verksamhetsutveckling och formuleras inte vid utvecklingen för att sedan kontrolleras innan system och rutiner tas i drift. Hanteringen av säkerhetsfrågorna är inte integrerad som en del i processen för system- och verksamhetsutvecklingen, vilket kan leda till att dessa beaktas först i efterhand med risk för avsevärda fördyringar eller med risk att inte beaktas alls.

I ledningens engagemang för säkerhetsfrågorna saknas ett mer systematiskt angreppssätt när det gäller prioriteringar och uppföljning, för att tydliggöra vikten av dessa frågor.

Riksrevisionen bedömer därför sammantaget att ledningens kontrollmiljö när det gäller informationssäkerhet har brister som främst rör de förutsättningar som ledningen skapat för informationssäkerhetsarbetet. Detta har hindrat kommunikation mellan aktörerna och samverkan mellan de olika delarna[19] i informationssäkerhetsarbetet. Vi noterar dock att ledningen under senare tid tagit initiativ till att få en bättre organisation för informationssäkerhetsarbetet.

[19] Riskanalys, prioritering, beslut om och införande av säkerhetsåtgärder samt uppföljning av dessa.

4 Riskanalys

4.1 Bedömningskriterier

Riskanalys är en viktig förutsättning för och del av myndighetens riskhantering. Arbetet med riskanalyser behöver **organiseras** och styras. Riskhanteringen innefattar en process för riskanalys. Den omfattar analyser och bedömningar av väsentliga hot, risker och konsekvenser av genomförda hot. För att bedöma om en verksamhet har genomfört en adekvat riskanalys kan sex olika kriterier användas.

Som underlag för analysen behövs identifiering[20] av de skyddsvärda informationstillgångarna. De bör dokumenteras i en överblickbar **förteckning** eller databas.

Åtminstone de tillgångar som är strategiska för verksamheten bör åsättas en beslutad säkerhetsnivå – **informations- eller säkerhetsklassning** – med hänsyn till verksamhetens krav på säkerhet så att en prioritering av säkerhetsåtgärder kan göras. Säkerhetsklassning av informationen i systemen och av andra informationstillgångar behövs för att kunna avgöra lägsta acceptabla säkerhetsnivå för dem.

Riskanalysen bör utföras med hjälp av beslutade och dokumenterade **metoder**[21]. Riskanalysen bör uppdateras årligen, och däremellan vid behov.

Analysen bör omfatta **alla typer av risker, dvs.** för bristande tillgänglighet, riktighet, sekretess och spårbarhet som kan vara väsentliga i verksamheten.

Det bör finnas en tydlig och uppföljningsbar **åtgärdsplan** som förtecknar beslutade säkerhetsåtgärder[22] för att möta de risker som framkommit i analysen. Planen bör beskriva när åtgärderna ska vara genomförda och vem som ansvarar för deras genomförande. I stora verksamheter kan det behövas flera åtgärds(del)planer. Det är då viktigt att det även finns en samlad åtgärdsplan som ledningen kan överblicka.

I riskanalysarbetet ingår att analysera **incidenter** för att på så sätt kunna skapa förutsättningar (säkerhetsåtgärder eller sätt att undvika dem) för att

---

[20] Identifieringen bör omfatta: Vilka de är, vem som är ägare/har ansvar för dem, var de finns samt vilka kopplingar till andra tillgångar respektive tillgång kräver när den används.

[21] Exempel på riskanalysmetoder är SBA Scenario, RiscPac, CRAMM, RA, ISAP, ISF Sprint och Proteus.

[22] Det vill säga nya skyddsåtgärder för att uppfylla specificerade säkerhetskrav som avser en viss informationstillgång. Exempel på sådana skyddsåtgärder är organisation och ansvar för säkerhet, administrativa rutiner, personalsäkerhet, fysiskt skydd, driftrutiner samt utrustnings- och programvarubaserade funktioner. Åtgärderna kan även indelas i förebyggande skydd, detekterande skydd och återställningsrutiner.

begränsa dem i framtiden. Incidenter bör systematiskt dokumenteras och rapporteras så att en bild av de upptäckta säkerhetsproblem som finns i myndighetens informationshantering kan skapas.

4.2 Iakttagelser

Försäkringskassan har beslutat om regler för arbetet med analys av informationssäkerhetsrisker. Enligt reglerna ska regelbundna (årliga) risk- och sårbarhetsanalyser göras.

Säkerhetschefen genomför riskanalyser enligt förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, krisberedskapsförordningen samt enligt förordningen (1995:1300) om myndigheters riskhantering.

Verksamhetsansvarig chef eller IT-produktägare ansvarar för att verksamheten belyses årligen i en risk- och sårbarhetsanalys.

System- och produktansvariga (dvs. systemägaren eller den som mottagit delegation från denne) ska genomföra analys av säkerhetsbehov med hänsyn till systemens informationsinnehåll och verksamhetens krav.

Vid Försäkringskassan finns det åtskilliga förteckningar över skilda typer av tillgångar (objekt såsom databaser, IT-system, system- och driftdokumentation, programlicenser m.m.). Det finns emellertid ingen överblickbar samlad **förteckning** eller databas över skyddsvärda objekt och de med respektive objekt förknippade hoten, genomförda skyddsåtgärder och kvarstående sårbarheter. Försäkringskassan indelar sina tillgångar i verksamheten i tre grupper – IT-driftcentralen i Sundsvall, IT-systemen och personalen – men man saknar hjälpmedel att bryta ned dessa grova kategorier. Utan systematisk nedbrytning i övervägda underkategorier finns det risk för att väsentliga informationstillgångar inte kommer att identifieras, analyseras och därmed få ändamålsenligt skydd.

Säkerhetsklassning av informationen i systemen och andra informationstillgångar tillämpas i liten utsträckning trots att detta ska ske enligt de egna riktlinjerna för informationssäkerhet. Ett rådande synsätt är att all information i socialförsäkringen är lika skyddsvärd och att IT-systemen som behandlar den är så starkt kopplade till varandra att om ett IT-system upphör att fungera så upphör också de andra systemen att fungera. Informationen säkerhetsklassas därför inte.

Försäkringskassan har ingen gemensam, beslutad uppsättning **metoder** för analys av olika typer av risker i syfte att styra kvalitet och jämförbarhet i riskanalyserna. I riktlinjerna för informations-säkerhet konstateras endast att två metoder förekommer, inte i vilka fall de ska användas.

Under intervjuerna har det framkommit exempel på att alla **risker** inte behandlats tillfredsställande i Försäkringskassans riskanalyser. Bedömning av sannolikheten för interna antagonistiska hot från personal som blir övertalig till följd av det pågående förändringsarbetet har inte gjorts. Några överväganden om skyddsåtgärder med anledning av detta hot har följaktligen inte gjorts. Ett annat exempel utgörs av en allvarlig incident som ledde till långvarigt avbrott i Försäkringskassans arbete över landet. Den inträffade till följd av bl.a. bristande analys av riskerna förknippade med underhållsrutinerna[23] för operativsystemen. Ett ytterligare exempel avser Försäkringskassans beroende av tillgång till information från andra myndigheter. Det görs ingen samlad analys som belyser riskerna hos de levererande myndigheterna och hur detta skapar risk hos Försäkringskassan. Risken för att någon extern informationsöverföring till Försäkringskassan inte kommer till stånd eller innehåller fel studeras alltså inte på ett tillräckligt systematiskt sätt. Detta senare exempel indikerar även brister i Försäkringskassans omvärldsbevakning och i systematiken i riskanalysarbetet.

Det finns även exempel på risker som är en direkt följd av Försäkringskassans eget agerande och som inte analyseras på ett metodiskt sätt. Ett sådant exempel är de risker som uppstår till följd av den stora mängden system och de komplexa sambanden (kopplingarna) som råder mellan dem. Risker uppstår på grund av bristande möjligheter för analytikerna att överblicka[24] hur incidenter i ett visst system påverkar andra system. Detta hindrar eller försvårar att risker upptäcks och åtgärdas på ett bra sätt. Riskerna förknippade med underhållsrutinerna för operativsystemen som nämnts ovan är av detta senare slag.

Ett exempel på Försäkringskassans komplexa beroende av omvärlden är de beroenden som finns när det gäller utbetalning av ersättningar. I regleringsbrevet för 2005 understryks vikten av att Försäkringskassans kunder får ut sina ersättningar. Detta innebär att Försäkringskassan måste uppmärksamma risker, sårbarheter och säkerhetsarbeten även i omvärlden. Att behärska de interna riskerna för brister i de utbetalningsuppdrag som Försäkringskassan överför till bankerna räcker inte för att försäkra sig om att kunderna får ut sina ersättningar om bankernas utbetalningssystem slutar att fungera – utbetalningar kommer då ändå inte till stånd. Försäkringskassan kan inte ta ansvar för bankernas säkerhetsarbete, men medverkar i Krisberedskapsmyndighetens samverkansgrupp för ekonomisk säkerhet. I denna grupp har man sedan 2003 analyserat riskerna i samhällets

[23] Beskrivningen är avsiktligt översiktlig.

[24] Det saknas en helhetsbild över systemen som på ett överskådligt sätt kan återge bl.a. kopplingarna mellan (del-)systemen. Det försvårar bl.a. ett systematiskt arbete med prioritering av säkerhetsåtgärder där insikten om behovet och valet av åtgärd kan påverkas av kunskapen om hur systemen är kopplade till (dvs. påverkar) varandra.

betalningssystem. Analysarbetet har stött på betydande problem på grund av komplexiteten och är ännu inte slutförd.

Av intervjuerna framgår att behandlingen av säkerhetsrisker i systemutvecklingen inte sker tillräckligt systematiskt – dessa risker beaktas inte tillräckligt tidigt och tydligt i systemutvecklingsarbetet. Det nyutvecklade ärendehanteringssystemet ÄHS/FÄS förorsakade initialt betydande svårigheter för handläggarna genom att bl.a. riskerna för avbrott inte analyserats under utvecklingsprocessen. Avbrott och andra problem skapade ärendebalanser. Dessa problem har uppstått trots att driftsättningen uppskjutits vid ett tillfälle. Den bedömning av återstående risker för bl.a. bristande tillgänglighet som gjordes inför driftsättningen har alltså haft brister.

En del av det inom huvudkontoret bedrivna riskanalysarbetet avser såsom nämnts den riskanalys som ska utföras enligt förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, krisberedskapsförordningen. Den ställer krav på statliga myndigheter att årligen göra risk- och sårbarhetsanalyser och rapportera dessa till regeringen och Krisberedskapsmyndigheten. Någon dialog kring denna rapportering med regeringen eller Krisberedskapsmyndigheten sker dock inte. Säkerhetschefen gör de övergripande riskanalyserna som omfattar alla risker, dvs. också risker för personalen och för andra tillgångar än informationstillgångarna. Utgångspunkter är förändringar i det omgivande samhället och de hotbedömningar som Försäkringskassan får från bl.a. Krisberedskapsmyndigheten och i samband med möten inom de samverkansområdesgrupper som Krisberedskapsmyndigheten organiserar enligt förordningen[25]. Informationssäkerhetschefen och IT-säkerhetschefen gör riskbedömningar inom sina sakområden. Länskontoren deltar i mindre utsträckning i denna riskanalys. Av intervjuerna framgår att denna analys visserligen beskriver många av de största riskerna men att den inte på något sätt kan ersätta den samlade riskanalysen för hela verksamheten som behövs som grund för en ändamålsenlig åtgärdsplan. En sådan riskanalys saknas i dag.

Vidare genomförs riskanalys enligt förordningen (1995:1300) om myndigheters riskhantering. Säkerhetschefen har ansvar för genomförandet av denna. Senast analysen gjordes samlades verksamhetsansvariga chefer inom Riksförsäkringsverket till en workshop med stöd från personal från Kammarkollegium. Analysen har utförts vart tredje år enligt Kammarkollegiums anvisningar. Denna riskanalys lämnas aldrig till regeringen.

[25] Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap: 4 § Myndigheterna som anges i bilagan till denna förordning ska planera och vidta förberedelser för att förebygga, motverka och begränsa identifierad sårbarhet och risker inom de samverkansområden som anges i bilagan.

Analysen inriktas[26] mot risker vars negativa följder är ekonomiskt mätbara. Inte heller denna analys ersätter en samlade riskanalys.

Därutöver gör Försäkringskassan centralt analyser ad hoc på avgränsade områden – exempelvis telefoni – som vid skilda tillfällen bedöms som intressanta. Sådana analyser kan initieras av säkerhetschefen eller GD. Ibland görs de på initiativ av verksamhetsansvariga chefer utifrån deras egna behov. Av intervjuerna framgår att de risker som inom Försäkringskassans ledning betraktas som väsentliga för närvarande är risken för pandemi, personal som gör misstag i handläggningsarbetet och i arbetet med systemdriften samt ”IT-hotet”. Med ”IT-hotet” avses virusattacker med allvarliga konsekvenser samt angrepp via Internet på systemen från missnöjda kunders sida. Denna centralt bedrivna analysverksamhet bedrivs enligt uppgift utan enhetliga former beträffande organisation och metodik.

Riskanalys på länsnivå görs i huvudsak av länssäkerhetssamordnarna utan närmare styrning av länsledningarna. Det har tidigare även förekommit att riskanalyser beställts av RFV.

Frågor som fokuseras under 2005 i riskanalyser på länsnivå[27] är främst säkerhetsfrågor som berör personalens arbete med klienterna – riskerna för våld och hot samt brandskydd. En del informationssäkerhetsfrågor har tagits upp, bl.a. arkivsäkerhet och behörighetsadministration. Riskerna förknippade med några IT-system[28] har tidigare också analyserats. Länssamordnaren har träffar med länsdirektören, men någon formaliserad och dokumenterad rapportering sker inte. Beträffande incidenter överlämnas dock regelbundet statistik till länsdirektören. Riskanalysarbetet på länsnivå varken stöds eller styrs från huvudkontoret. Det sker ingen uppföljning av kvaliteten hos riskanalyserna som bedrivs i länen. Inte heller sker någon utbildning i metoder.

Försäkringskassans **incidentrapportering** har i riktlinjerna getts en detaljerad beskrivning. Såsom den tillämpas har emellertid rapporteringen och hanteringen av incidenter haft flera brister. Frågan huruvida rapporteringen är rättvisande belyses av att två av länskontoren inte rapporterat in någon incident alls under 2004. Enligt intervjuerna är detta ett tecken på brister i inrapporteringen. När det gäller hanteringen av rapporterade incidenter är denna lokal på så sätt att incidenter som rapporteras inom länet också hanteras inom länet; de delges inte huvudkontoret annat än i statistisk form. Detta försvårar erfarenhetsåterföring och inlärning baserad på inträffade incidenter i den samlade verksamheten.

Som redan påpekats i kapitel 3 har ingen fått ett tydligt utpekat ansvar för att göra eller sammanställa en samlad riskanalys beträffande

---

[26] Enligt information (2005-01-01) från Kammarkollegium.

[27] Som redan nämnts grundas våra iakttagelser beträffande länsnivån på intervjuer på ett mycket stort och ett litet (s.k. 3 %-kassa) länskontor.

[28] Till exempel har Agresso, vissa PA-system samt Invoice Manager enligt uppgift analyserats.

informationssäkerhet för Försäkringskassan. Med samlad riskanalys menas här en från verksamheterna underbyggd (nedifrån-upp) riskanalys. Det innebär bl.a. att det vid sidan av resultatet från den förenklade riskanalysen enligt krisberedskapsförordningen – till den del som avser informationssäkerhet – inte finns någon egentlig överblick över risknivån i skilda verksamheter och hur de skiljer sig åt sinsemellan. De skilda riskanalyser som genomförs på olika nivåer i Försäkringskassan kan inte överblickas så att exempelvis risknivåer i skilda verksamheter kan jämföras.

Inte heller har någon fått ett tydligt ansvar för att sammanställa alla enskilda åtgärdsplaner inom informationssäkerhetsområdet till en överblickbar samlad **åtgärdsplan** som förtecknar beslutade nya informationssäkerhetsåtgärder, ansvariga för deras genomförande och kostnaderna för detta.

4.3 Bedömning

Försäkringskassans arbete med att analysera risker för informationssäkerheten har flera viktiga brister i jämförelse med normen.

En brist är avsaknad av organisering och styrning av samlade analyser av informations- och IT-säkerhetsrisker för Försäkringskassan som helhet. Verksledning och verksamhetschefer på huvudkontoret saknar även enligt vår bedömning tillräckligt stöd och hjälpmedel för att skapa en rättvisande och överblickbar bild över riskläget i enskilda försäkringsslag/produkter och länskontor, när det gäller typ av risk m.fl. aspekter. Denna brist på möjligheter att överblicka och jämföra riskerna bedömer Riksrevisionen medför bl.a. svårigheter för myndighetsledningen att avgöra om beslutade säkerhetsåtgärder inom skilda verksamheter är i linje med av riksdag och regering beslutade normer (lagar och förordningar) eller av verksledningen fattade övergripande beslut. Ett sådant beslut utgör Riksförsäkringsverkets beslut[29] från 2001 att längre avbrottstider än 24 timmar inte kan accepteras. Verksledningen har inte heller möjlighet att överblicka utestående[30] risker och hur hanteringen av dessa utvecklas över tiden.

Med reservation för granskningens omfattning på länsnivå[31] bedömer Riksrevisionen att riskanalysarbetet har svaga kopplingar mellan central och lokal nivå, när det gäller styrning från central nivå och rapportering från länsnivån. Brister finns även när det gäller styrning och rapportering inom länsnivån.

---

[29] Detta beslut kvarstår oförändrat i den nya organisationen.

[30] Med utestående risker avses risker som Försäkringskassan valt att inte skydda sig för, och alltså medvetet tar. Bakgrunden kan vara att skyddskostnaderna anses för höga eller incidenter alltför osannolika.

[31] Riksrevisionen har endast studerat riskanalysarbetet på länsnivå i två länskontor och kan därför inte dra några säkra slutsatser om generella förhållanden i de 21 länskontoren.

En annan brist avser riskanalysarbetets förutsättningar när det gäller omvärldsbevakning. Till exempel saknas en samlad bedömning av riskerna för brister i överföring av information till Försäkringskassan från andra myndigheter.

Riksrevisionen bedömer att de brister som framkommit ovan innebär att Försäkringskassan saknar en sammanhängande, systematisk och dokumenterad riskanalysprocess. Dessa brister försvårar verksledningens arbete och kan därigenom påverka kvaliteten i ledningsarbetet inom informationssäkerhetsområdet. Konsekvenserna kan bli både förhöjda informationssäkerhetsrisker och risker för att Försäkringskassan ådrar sig onödiga kostnader för sin informationssäkerhet.

5 Ledningens kontrollfunktioner samt införda skyddsåtgärder

5.1 Bedömningskriterier

Med kontrollfunktioner avses i detta sammanhang de åtgärder som ledningen utformat för att förebygga, upptäcka och åtgärda brister i informationssäkerheten. Dessa kan exempelvis vara att formulera och införa styrdokument och regler som avser informationssäkerheten och tekniska kontrollåtgärder såsom behörighetskontroller, loggnings-förfaranden m.m. Kontrollfunktionerna utgör sammantagna en väsentlig del av myndighetens ledningssystem för informationssäkerhet (LIS).

Myndigheten bör ha ett LIS med **beslutade och dokumenterade komponenter.** LIS syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra informationssäkerheten. Ett väl fungerande LIS innebär därmed att de strategiska informationstillgångarna har ett tillräckligt och kostnadseffektivt skydd i förhållande till bedömda risker.

LIS bör normalt ha följande **omfattning** när det gäller komponenter[32]:

- Informationssäkerhetspolicy,
- process för incidentrapportering inklusive beslut om vilka incidenter som ska rapporteras till ledningen,
- åtgärdsplan för informationssäkerhet,
- kontinuitetsplan,
- utsedd person med övergripande och samordnande ansvar för myndighetens informationssäkerhet,
- Internetpolicy,
- distansarbetspolicy,
- e-postpolicy,
- åtkomstpolicy[33],
- process för säkerhetskopiering av all verksamhetskritisk information,
- process för styrning av utveckling/förändringar i IT-miljö, IT-system och bemanning,

[32] En del komponenter tas upp i särskilda avsnitt, bl.a. riskanalys och de som avser utbildning och information, och medtas därför inte i denna uppställning.

[33] Policy som reglerar åtkomst av informationstillgångar.

- tekniska skyddsåtgärder (behörighetskontrollsystem, virusskydd, brandväggar m.m.),
- processer för att kontrollera efterlevnaden av det regelverk för upprätthållande av informationssäkerhet som bl.a. ovannämnda policykomponenter tillsammans bildar,
- en till all personal kommunicerad skriftlig beskrivning av roller[34] i informationssäkerhetsarbetet och hur ansvar och befogenheter för myndighetens informationssäkerhet fördelats på dessa,
- processer för återkommande uppföljning och förvaltning av LIS.

Komponenterna bör vara utformade utifrån myndighetens särskilda behov och därvid beakta relevant **best practice**[35] inom aktuellt område.

De bör vidare vara väl **införda** i verksamheterna.

Komponenterna bör tillsammans utgöra en lämpligt utformad **helhet** genom sina inbördes samband samt utgöra en väl integrerad del i myndighetens (totala) ledningssystem.

5.2 Iakttagelser

Försäkringskassans utgångspunkter för sitt LIS-arbete är standarden ISO 17799 i kombination med KBM:s vägledning BITS (baskrav för IT-säkerhet).

Granskningen visar att Försäkringskassan har ett LIS med **dokumenterade och beslutade komponenter**. De delar av ett LIS som införts omfattar övergripande policydokument och riktlinjer, ansvarsfördelning och organisation, rutinbeskrivningar för vissa delar av säkerhetsarbetet samt ett flertal tekniska säkerhetsåtgärder som ingår i myndighetens IT-infrastruktur. Det finns dock brister i vissa komponenter och andra saknas, vilket framgår nedan.

Styrande interna dokument för informationssäkerheten är främst arbetsordning, säkerhetspolicy och riktlinjer för informationssäkerhet. Mer preciserade riktlinjer för IT-systemen/IT-produkter avser kontinuitetsplaner för IT-system, systemsäkerhetsplaner och systemförvaltningsplaner med beskrivningar av åtgärder som avser informationssäkerhet. Vidare finns rutinbeskrivningar för incidenthantering, hantering av personuppgifter, säker arbetsplats, in- och utloggning på arbetsplatser, arbete på resa, användning av Internet, distansarbete, virusskydd, användning av e-post i tjänsten, service/avveckling av IT-utrustning, utplåning av IT-medier som innehåller information samt skydd mot stöld av IT-utrustning. Merparten av dessa

[34] Exempelvis säkerhetschef, systemägare, användare, IT-styrgrupp m.fl.

[35] Myndigheten bör alltså informera sig om och dra nytta av de kunskaper som finns i standarder såsom SS-ISO/IEC 17799, NIST:s 800-serie av rapporter.

policydokument och riktlinjer finns tillgängliga på Försäkringskassans intranät.

Viktigare tekniska säkerhetsåtgärder är reservanläggning för IT-drift (alternativ datorhall), behörighetssystem, övervakningssystem, säkerhetskopiering av information, IT-stöd för rapportering och analys av incidenter, kryptering samt helpdesk.

Det finns en organisatorisk enhet som har ett särskilt ansvar för informationssäkerhetsfrågor.

Även om Försäkringskassan har infört åtskilliga säkerhetsåtgärder, såsom ansvarsfördelning och regler, visar granskningen på vissa brister i **införandet** av LIS och att LIS inte i tillräcklig utsträckning fungerar utifrån **best practice**.

Försäkringskassan och dess föregångare har under de senaste tre åren gjort många informationssäkerhetssatsningar. De har avsett bl.a. ett bättre behörighetssystem, utbildning av personal, incidentrapportering och en ny alternativ datorhall. Det finns dock ingen samlad dokumenterad överblick över införda säkerhetsåtgärder eller någon överblick över behovet av att införa nya skyddsåtgärder (samlad åtgärdsplan) på central och lokal nivå samt inom IT-verksamheten. Överblicken av behovet av säkerhetsåtgärder sett över hela Försäkringskassan saknas därmed samtidigt som risken för dubblerade investeringar ökar.

Även om ledningen därmed inte har tillräcklig överblick över säkerheten totalt sett, dvs. om säkerhetsnivån uppfyller beslutade krav, finns ändå krav på säkerhet och överblick av säkerhetsåtgärder för enskilda IT-produkter, IT-system etc. Av dokumentet Riktlinjer för informationssäkerhet[36] samt av särskild rutinbeskrivning för systemsäkerhetsplaner[37] har Försäkringskassan, och tidigare RFV, bedömt att s.k. systemsäkerhetsplaner är en viktig säkerhetsåtgärd på systemnivå. Sådana planer ska enligt riktlinjerna finnas för varje IT-system och omfatta alla säkerhetskrav för systemet i fråga. De säkerhetskrav som anges ska vara uppfyllda innan produkten/systemet börjar användas. Granskningen visar dock att sådana systemsäkerhetsplaner endast finns för ett system och att den planen dessutom är inaktuell. Såväl den tidigare som den nuvarande ledningens beslut om denna säkerhetsåtgärd har alltså inte blivit genomförd. Det har ej heller framkommit till ledningen att så var fallet.

Försäkringskassan har många verksamheter, en komplex IT-arkitektur och tydliga krav från riksdag och regering på att kunna fungera under påfrestningar i fredstid. Detta ställer krav på att säkerhetsåtgärder införs som motsvarar dessa krav. Behovet av att kontinuerligt följa upp att åtgärderna

[36] Februari 2005.
[37] 2003.

uppfyller säkerhetskraven är därmed en fråga av stor vikt. Sådana uppföljningar kan anges i en särskild övergripande uppföljningsplan, där det anges vad som ska följas upp, för vem, när, hur och av vem uppföljning ska genomföras. En sådan plan eller annat arrangemang[38] som säkerställer uppföljning av att säkerhetsåtgärderna uppfyller ställda krav finns inte inom Försäkringskassan. En förutsättning för en sådan plan är att den kan grundas på en översikt över vidtagna, beslutade och planerade säkerhetsåtgärder (investeringar i säkerhet). En sådan översikt saknas. Detta hade sannolikt möjliggjort för ledningen att bli informerad om problemet med att införa systemsäkerhetsplanerna.

Innan ett IT-system tas i drift ska systemet säkerhetsgodkännas av produktägare och informationssäkerhetschefen. Dessa rutiner har inte fungerat tillfredsställande under hösten 2005 när Försäkringskassan driftsatte systemet ÄHS/FÄS[39]. Vid driftsättningen visade sig FÄS innehålla felaktigheter och att prestandan var för dålig. Handläggarna hade dessutom problem att hantera systemet. I intervjuerna framkom att orsakerna till driftsättningsproblemet är att krav på säkerhet inte tas upp tillräckligt tidigt i verksamhets- och systemutvecklingen. Den säkerhetsanalys som görs därmed är för begränsad och beaktar inte tillräckligt risker i den verksamhet där systemet ska användas.

De redovisade bristerna ovan innebär inte att Försäkringskassan helt saknar rutiner för att följa upp informationssäkerheten. Sådana finns exempelvis inom IT-avdelningen som varje månad tar fram en s.k. ”Statusrapport leverans”. Här ges information om releaser, utvecklingsprojekt (IT), efterfrågan på metodstöd m.m. Olika problem med leveranser av IT-tjänster beskrivs med riskbedömningar, riskkonsekvenser och förslag till åtgärder.

Även om inte IT-systemen har systemsäkerhetsplaner finns annan dokumentation med inslag av säkerhetsfrågor. Systemdokumentet Plan för affärsmässig förvaltning (förvaltningsplan) omfattar bl.a. ett s.k. Service Level Agreement (SLA). Vidare finns dokumenten Driftdokumentation respektive Månadsrapport. Sammantaget kan dokumenten ge en uppfattning om säkerhetskrav för enskilda IT-system vad gäller tillgänglighet till systemen och i viss mån säkerhet beträffande informationens integritet genom kraven på backup-rutiner. Avbrotts- och katastrofsituationer tas också upp.

Försäkringskassan har en incidentrutin och incidenthanteringsorganisation. Som påpekats tidigare finns det kvalitetsproblem med nuvarande rutin för incidentrapportering. Säkerhetschefen uttalar i en intern PM (2005)

[38] På annat sätt skapad och kommunicerad överblick över uppföljningsarbetet.

[39] System för handläggning av tillfällig föräldrapenning.

med sammanställning av incidenter under 2004 att kvaliteten i inrapporteringen av incidenter varierar för mycket mellan lokala kassor. Detta medför svårigheter att dra rättvisande slutsatser av incidentdata. Incidentrutinen har således inte blivit tillräckligt väl införd i organisationen.

Försäkringskassan har aktiviteter för att bevaka hoten i omvärlden. Virusattacken våren 2004 visade att den interna rapporteringen av potentiella hot inte fungerade tillfredsställande. Trots att virushotet var känt inom IT-organisationen, fördes inte information om hotet upp på ledningsnivå för bedömning och beslut om åtgärd.

När virusattacken inträffade rapporterades den som en mycket allvarlig incident. Det medförde att krisorganisationen trädde i kraft. I efterhand visade internrevisionen på ett flertal brister i bl.a. krisorganisationen och möjligheterna att kommunicera under hanteringen av incidenten. Myndigheten har därefter vidtagit åtgärder för att få krisorganisationen att fungera bättre.

Specifika säkerhetsåtgärder som saknas i jämförelse med LIS-standarden är de verksamhetsansvarigas återkommande uppföljning av användarnas riskmedvetande och kompetens att hantera informationssäkerhetsriskerna samt processer för återkommande uppföljning och förvaltning av komponenterna i LIS (riskanalyser, kontrollåtgärder, utbildning etc.).

5.3 Bedömning

Riksrevisionen konstaterar att Försäkringskassan uppfyller flera av kraven beträffande kontrollåtgärderna enligt LIS-standarden. De väsentliga styrdokumenten finns på plats. Riktlinjer finns för säkerheten inom viktiga områden. Flera tekniska säkerhetsåtgärder, som man kan förvänta sig i en sådan omfattande och betydelsefull IT-infrastruktur, finns införda. Det sker en fortlöpande uppföljning av vissa säkerhetsaspekter, främst tillgänglighet uttryckt i servicenivåer (SLA).

Även om väsentliga säkerhetsåtgärder finns införda är det Riksrevisionens slutsats att verksledningen inte har skapat de möjligheter/hjälpmedel till överblick som behövs för att ledningen ska kunna övertyga sig om att befintliga och beslutade säkerhetsåtgärder tillsammans hanterar säkerhetsbrister på ett för ledningen tillfredsställande sätt. På en övergripande nivå saknas en sammanhållen åtgärdslista för säkerhetsåtgärder och uppföljning av dessa åtgärder.

Införandet av Försäkringskassans säkerhetsåtgärder kan ifrågasättas utifrån vår granskning av den faktiska förekomsten av säkerhetsplanerna – en viktig byggsten i Försäkringskassans säkerhetsarkitektur. Ingen uppföljning av denna säkerhetsåtgärds funktion hade uppenbarligen gjorts.

Att ledningens bristande möjligheter till överblick tillsammans med uppföljningens brister skapar reella problem i form av bristande skydd för incidenter och möjligheter att hantera deras konsekvenser har enligt Riksrevisionens mening klart framgått. Nyligen inträffade allvarliga händelser[40] har indikerat att ledningens uppföljning av säkerheten inte varit tillräcklig.

Sammantaget bedömer Riksrevisionen att konstaterade svagheter i säkerhetsåtgärderna och uppföljningen av dessa leder till en förhöjd risk för brister i informationssäkerheten.

[40] Vi avser virusincidenten 2004 samt problem vid införandet av FÄS 2005.

6 Information och utbildning om informationssäkerhet

6.1 Bedömningskriterier

Området information och utbildning avser ledningens åtgärder för att förse personalen med relevant information och kunskaper om informationstillgångar, säkerhetsåtgärder, incidenter och andra viktiga aspekter beträffande LIS. Området innefattar också åtgärder för att säkra att ledningen får relevant information från organisationen om personalens kunskaper om informationssäkerhet.

Det bör finnas en **process** för systematisk och återkommande information och utbildning beträffande informationssäkerhet till **berörda personalgrupper**[41]. Den bör innefatta de anställdas ansvar för informationssäkerheten samt de väsentliga hot och risker som ska beaktas i deras arbete. Syftet med informations- och utbildningsåtgärderna bör vara att ge all berörd personal förutsättningar att hantera sådana informationssäkerhetshändelser som kan uppkomma.

6.2 Iakttagelser

Enligt Försäkringskassans styrdokument är respektive verksamhetschef ansvarig för att personalen får säkerhetsutbildning som är relevant för de aktuella arbetsuppgifterna. Detta gäller även inom området informationssäkerhet. Cheferna ska ge personalen förutsättningar att inhämta kunskap om säkerhet. Vidare ingår i verksamhetsansvaret uppföljning och kontroll av hur säkerhetspolicyn efterlevs. Det är vidare var och ens ansvar att ta del av anvisningar och regler för säkerhet. Alla ska känna till säkerhetspolicyn, riktlinjerna och rutiner för informationssäkerhet. Varje person ska följa de regler som anvisas av ledningen.

Det åligger informationssäkerhetschefen enligt riktlinjer för informationssäkerhet att följa upp utbildningsstatus och riskmedvetande inom myndigheten. I riktlinjerna för informationssäkerhet definieras området och viktiga begrepp anges. Vidare anges att säkerhetsinformation och utbildning syftar till att uppnå och upprätthålla säkerhetsmedvetenhet. Enheten för

[41] Personal med ansvar för säkerhet, nyanställda, myndighetsledning, övriga chefer, övriga medarbetare.

informationssäkerhet har ett ansvar för att sprida information och ta fram utbildning inom området.

Enligt riktlinjerna för informationssäkerhet är genomgång av säkerhetsfrågor med **berörda personalgrupper** obligatorisk vid nyanställning, övergång till annan tjänst samt vid behörighetstilldelning, t.ex. för ett specifikt IT-system. Vidare ska verksamhetsansvarig tillse att anlitade konsulter får tillräcklig information och utbildning om informationssäkerhet. Informationssäkerhetsenheten har tagit fram en särskild utbildning i informationssäkerhet, s.k. e-baserad säkerhetsutbildning, som riktar sig till all personal.

Information om säkerhetsregler på intranätet

Försäkringskassan informerar de anställda om de interna regler som gäller informationssäkerhet på intranätet. Här finns säkerhetsorganisation och rutiner tillgängliga liksom de interna regeldokumenten (t.ex. arbetsordning, säkerhetspolicy och riktlinjer för informationssäkerhet).

Säkerhetsutbildning

Granskningen visar att dåvarande Riksförsäkringsverket år 2003 bedömde det som nödvändigt att allmänt höja medvetenheten om säkerhetsfrågor, bl.a. informationssäkerhet. Enheten för informationssäkerhet tog fram den e-baserade utbildningen, vilken genomfördes av ca 90 % av de anställda under åren 2004 och 2005. Utbildningen omfattar: Introduktion, Personsäkerhet, Fysisk säkerhet, Grundutbildning i informationssäkerhet, Chefens ansvar och Informationssäkerhet vid systemutveckling. Varje utbildning tar c:a 30 minuter och har skett i distribuerad form basera på interaktiva självstudier på Försäkringskassans intranät eller CD-skiva.

Cheferna vid Riksförsäkringsverket fick återkommande muntlig utbildning i säkerhetsfrågor. Någon sådan insats har inte gjorts i Försäkringskassan under 2005.

Även om Försäkringskassan genom en ”engångsinsats” genomfört en nödvändig höjning av medvetenheten finns inte en systematisk utbildningsverksamhet och -**process** införd.

Försäkringskassan har ingen utbildning (motsvarande) som riktas specifikt till ledningsgruppen eller myndighetens styrelse. Styrelsen har fått information som rör vissa delar av säkerheten, såsom den nybildade säkerhetsstaben och allvarliga incidenter.

Det finns ingen systematisk ansats att utbilda säkerhetspersonal i syfte att nå en mer enhetlig uppfattning om vad arbetet med informationssäkerhet på olika nivåer i organisationen innebär och med vilka metoder det ska bedrivas. Utöver den generella utbildning som alla anställda getts tillfälle att genomgå, bör de som arbetar med säkerhetsfrågor genomgå systematiskt upplagd utbildning i syfte att uppnå en mer enhetlig syn på frågorna. Ett

exempel på ett sådant utbildningsbehov är att utbilda i hur man genomför riskanalyser, vilket de lokala säkerhetsombuden behöver för att kunna vara det stöd till verksamhetsansvariga som organisationen förutsätter.

Uppföljning och kontroll av medvetenhet om informationssäkerhet

Ansvaret för uppföljning och kontroll av att personalen följer de regler som angetts av ledningen åvilar som nämnts verksamhetsansvariga. Granskningen visar att verksamhetsansvariga följer upp att personalen har rätt behörighet för aktuella arbetsuppgifter. Någon uppföljningsplan för säkerhetsmedvetandet finns inte[42].

6.3 Bedömning

Försäkringskassan har under senare tid förbättrat informationen om och utbildningen i regler och åtgärder för informationssäkerhet. Viktiga dokument finns tillgängliga via intranätet och en särskild e-baserad utbildning har tagits fram och genomförts för ca 90 % av personalen.

Försäkringskassan saknar en systematisk utbildningsverksamhet för verksamhetsansvariga chefer – de som är ansvariga för säkerheten – och för säkerhetspersonal.

[42] Försäkringskassan avser att införa en kompetensportal i intranätet vilket ger möjlighet för chefer att exakt se vilka utbildningar som personalen genomgått.

7 Uppföljning och förvaltning

7.1 Bedömningskriterier

Den snabba förändringstakten i omvärlden och i de egna verksamheterna kräver kontinuerlig omvärdering av processer och system för intern styrning och kontroll. Ledningens uppföljning av den interna styrningens och kontrollens utformning och effektivitet är vidare det kanske viktigaste underlaget för förbättring av myndighetens LIS.

Uppföljningen bör ske **systematiskt och regelbundet.** Den bör vara **dokumenterad.** Den bör åtminstone besvara om följande väsentliga delar i LIS fungerar som avsett:

- Kontrollmiljön: beslutade **delegationer**
- Riskanalys: riskanalysprocess och åtgärdsplanering
- Kontrollfunktioner och skyddsåtgärder:
  - Genomförande av åtgärdsplanerna,
  - Incidentrapporteringen,
  - Kontinuitetsplaneringen,
  - Den interna kontrollen av utveckling/förändringar i IT-miljö, IT-system och bemanning,
  - Den interna kontrollen av tekniska skyddsåtgärders funktion (behörighetskontrollsystem, virusskydd, brandväggar m.m.),
  - Om den faktiskt uppnådda informationssäkerheten systematiskt prövas och uppfyller säkerhetskraven,
- Information/utbildning: den interna kontrollen beträffande information och utbildning angående informationssäkerhet och den interna kontrollen av efterlevnaden av det regelverk för upprätthållande av informationssäkerhet som grundas på informationssäkerhetspolicy, Internetpolicy, e-postpolicy, distansarbetspolicy m.fl.

Resultaten från denna uppföljning och kontroll utgör underlag för förvaltning och utveckling av myndighetens LIS. Ledningen bör ha infört en dokumenterad process för förvaltning och utveckling av sitt LIS.

7.2 Iakttagelser

Kontrollmiljön

Det finns inget särskilt dokument av karaktären riktlinjer för vidareutvecklingen av LIS som grund för förändringsarbetet. Enligt uppgift ska en uppföljningsplan tas fram när den nya säkerhetschefen tillträder i början av 2006.

Säkerhetschefen utför ingen organiserad uppföljning av LIS, vilket inte heller tydligt ingår i ansvaret. Arbetsordningen talar om samordning, utfärdande av riktlinjer för säkerheten och stöd till säkerhetsfunktionerna. Säkerhetschefen har inga befogenheter att på eget initiativ kontrollera företeelser i linjen beträffande informationssäkerhetsfrågor. Den uppföljning som sker från säkerhetschefens sida är inte formaliserad och inte heller dokumenterad.

Informationssäkerhetschefen och IT-säkerhetschefen har däremot ett uppföljningsansvar enligt styrdokumenten, och det följer då av säkerhetschefens samordnande funktion att när något allvarligt inträffat ska detta rapporteras till säkerhetschefen. Det är alltså huvudsakligen[43] frågan om reaktiv rapportering – dvs. rapportering baserad på inträffad händelse.

Det finns inga avrapporteringsrutiner för uppföljning och utvärdering av LIS i sig.

Verksledningen följer upp sina **delegationer** beträffande informationssäkerhet vid träffar 7– 8 gånger om året med säkerhetschefen. Man går då igenom aktuella frågor. Säkerhetschefen har dock inget uppföljningsansvar[44] och kan, vid sidan av att rapportera incidenter, därför inte leverera en sammanhängande bild av verksamhetens arbete med informationssäkerhet.

Vid sidan av denna uppföljning skulle verksledningen rimligen också behöva återkommande orienteringar om utvecklingen och händelser i Försäkringskassans omvärld som skulle kunna påverka risksituationen. I vilken utsträckning säkerhetschefen kan delge en relevant bild därav genom egen omvärldsbevakning kan dock inte överblickas av verksledningen.

Riskanalysen

Försäkringskassan har inte kunnat visa att myndigheten systematiskt följer upp kvaliteten i riskanalyserna. Använda checklistor och tillämpningen av modeller och metoder som kommit till användning vid analyserna har inte heller följts upp.

---

[43] Informationssäkerhetschefen genomför dock en uppföljning i form av en självdeklaration till länsdirektörer och avdelningschefer.

[44] Detta är förändrat i och med beslutet den 27 januari.

Kontrollfunktioner och säkerhetsåtgärder

Uppföljning både lokalt och centralt brukar inom Försäkringskassan utlösas först då något allvarligt inträffat. Annars ges uppföljning av informationssäkerheten lägre prioritet bland flertalet chefer lokalt och centralt efter vad som framkommit i intervjuerna.

Försvarets radioanstalt har anlitats för dels penetrationstester, dels en säkerhetsgranskning av IT-plattformarna och av rutiner för hantering av säkerhetsbrister i programvaror och hårdvara.

Internrevisionen har gjort flera granskningar som berör skilda IT-system. Behörighetskontroll har varit en av de frågor som fokuserats i granskningarna. Uppföljning av behörigheter är för övrigt förknippad med stora svårigheter inom Försäkringskassan. För den gamla stordatormiljön finns ett sammanhållet behörighetskontrollsystem, men alla andra IT-plattformar[45] har sina egna behörighetskontrollsystem. Det innebär att det finns hundratals definierade behörigheter och att varje anställd kan ha flera tiotals behörigheter. Det försvårar självfallet uppföljningsarbetet på denna punkt.

Länsdirektörerna[46] är medvetna om sitt uppföljningsansvar i säkerhetsfrågor, bl.a. eftersom detta berörts på chefsutbildningarna då exempelvis uppföljning av medarbetarnas hantering av sina behörighetskort tagits upp. Trots detta görs systematisk uppföljning i liten utsträckning. Från huvudkontoret har det inte heller kommit några anvisningar eller tydliga krav på uppföljningsarbetet.

För närvarande har cheferna de lokala säkerhetssamordnarna som stödresurs för uppföljningsarbetet. Dessa har – med undantag för de största länskontoren – sin stöduppgift som tillikauppgift och delar sin arbetstid mellan flera länskontor.

De frågor som står i fokus för länssamordnarnas säkerhetsarbete är lås- och larmfrågor och andra frågor knutna till den fysiska säkerheten/personalens säkerhet. Detta beror enligt intervjuerna på incidenter som inneburit hot mot kassornas personal. Uppföljning av informationssäkerheten har däremot med vissa undantag (vissa loggkontroller, se nedan) inte kommit till stånd.

Länsdirektörerna ställer inga tydliga krav på länssäkerhets-samordnarens uppföljningsarbete. I informella samtal delger länssäkerhetssamordnaren enligt uppgift det som denne anser att länsdirektören bör få del av. På det sättet får länsdirektören främst information om incidenter av skilda slag,

[45] Försäkringskassan arbetar nu med att införa rollbaserade behörigheter vilket avsevärt förväntas förenkla tilldelningen och uppföljningen av behörigheter genom att antalet behörigheter reduceras samtidigt som de standardiseras.

[46] Som redan nämnts grundas våra iakttagelser beträffande länsnivån på intervjuer på ett mycket stort och ett litet (s.k. 3 %-kassa) länskontor.

bl.a. driftavbrott och andra felaktigheter i systemen. På det ena länskontoret tas även planerade säkerhetsåtgärder upp.

Vid kassorna finns ett stort intresse av att kontrollera att medarbetarna inte kommer åt information de inte har rätt att ta del av (t.ex. information om sig själva, närstående m.m.). Utöver de informella samtalen med säkerhetssamordnarna beställer länsdirektörerna årliga kontroller av loggar i syfte att kontrollera personalens åtkomst till informationen.

Information om och utbildning i LIS

Dåvarande Riksförsäkringsverket gjorde 2003 bedömningen att medvetenheten behövde höjas. Det åligger också informationssäkerhetschefen och IT-säkerhetschefen att följa upp medvetenheten. Primäransvaret för uppföljning har de verksamhetsansvariga. Granskningen visar att Försäkringskassan inte genomfört systematiska insatser för att kontinuerligt bedöma personalens säkerhetsbeteende och behov av ytterligare utbildning och information.

System för uppföljning, utvärdering och förvaltning av LIS

Det finns ingen övergripande plan för uppföljningen av säkerheten inom Försäkringskassan i vilken verksledningen beslutar vilken uppföljning som ska företas på skilda nivåer i organisationen och hur resultaten ska vidarerapporteras och sammanställas till verksledningen.

Någon övergripande granskning[47] av hur väl LIS fungerar har inte gjorts. Någon kontroll av uppföljningsarbetet på länsnivå har inte skett.

Uppföljningar av viktiga delar av LIS saknas också till stor del. Uppföljning av riskanalys, kontinuitetsplanering (utöver de frågor som rör IT-driften), policy för e-posthantering, policy för distansarbete, samt åtgärdsplaner[48] är alla viktiga delfunktioner i LIS vars funktion inte följs upp.

Försäkringskassans uppföljning och förvaltning av komponenterna i sitt LIS bygger enligt uppgift på att behov av förändringar och vidareutveckling av LIS behandlas och beslutas i verksamhetsplaneringen. Besluten kan avse omvärldsanalys, ändringar i arbetsordning, organisationsförändringar, ansvarsförändringar, nya modeller och metoder samt nya säkerhetskrav med anledning av konstaterade risker och sårbarhet kopplade till informationssäkerhet. Även om sådana aspekter på LIS hanteras i verksamhetsplaneringen avrapporterar inte de olika säkerhetsfunktionerna sina resultat i förhållande till de mål som gällt för året.

[47] Frågorna kring ansvarsfördelning har dock utretts som underlag för beslutet i januari 2006.

[48] Distansarbetspolicy och samlad åtgärdsplan finns inte och inte heller lokala/länsvisa åtgärdsplaner.

7.3 Bedömning

Enligt Riksrevisionens mening saknar Försäkringskassan en välutvecklad strategi för hur kvaliteten i LIS ska upprätthållas och vidareutvecklas utifrån en helhetsbild över bristerna i LIS. Detta innebär inte att åtgärder inte företas för att förändra LIS. Beredning och beslut om åtgärder för att utveckla delar av LIS sker i verksamhetsplaneringen men inte utifrån en sådan helhetsbild.

Uppföljningen av informationssäkerheten är endast delvis organiserad i nuläget. Någon övergripande och samlad uppföljning för att styrka att LIS fungerar som ett sammanhållet[49] system på ett bra sätt har inte gjorts. Den uppföljning som finns avser främst enskilda säkerhetsåtgärder, t.ex. uppföljning av intern åtkomst av information (behörighetskontroll) samt dokumentet Riktlinjer för informationssäkerhet, men inte implementeringen av riktlinjerna.

En viktig brist avser kommunikationen i uppföljningsfrågor mellan länskontoren och central nivå. Det finns riktlinjer för uppföljande kommunikation mellan länskontoren och huvudkontoret. Informationsutbytet kommer dock till stånd endast i mycket begränsad utsträckning. Någon samlad bild av hur bl.a. LIS fungerar i denna stora organisation kan därför svårligen skapas.

Ledningens uppföljning av informationssäkerheten är i huvudsak reaktiv och händelsestyrd. De proaktiva inslagen – dvs. uppföljning av de beslutade åtgärderna och deras genomförande – är sparsamt förekommande. Verksledningen bedöms därför inte ha tillräckligt underlag för att göra en tillförlitlig uppföljning av gjorda delegationer.

En allvarlig incident inträffade 2004 då virus tog sig in i nätverket (WANet[50]) och verksamheten lamslogs under 2 dagar. Det visade sig vid genomgången att den rutin som finns för att införa rättelser i operativsystemet som tillverkaren utfärdat för att ta hand om sårbarhet i detta system (patchhanteringsrutinen[51]) inte fungerat som tänkt och att dess funktion inte följts upp. Enligt Riksrevisionens mening är denna incident ett exempel på hur brister i uppföljningen av LIS funktion kan bidraga till att incidenter kan få allvarliga konsekvenser.

Sammantaget är Riksrevisionens bedömning att uppföljningen av LIS brister i systematik och regelbundenhet och att dessa brister medför förhöjd risk för bristande informationssäkerhet.

---

[49] Därmed menas att följa upp att alla ledningssystemets komponenter (riskanalys etc.) enskilt bidrar på avsett sätt och att den information som ska kommuniceras mellan komponenterna faktiskt överförs på avsett sätt.

[50] Wide Area Network.

[51] Rutinen ser till att den kod som leverantörerna av operativsystem och standardprogramvara utfärdar utan dröjsmål införs i syfte att täppa till sårbarhet.

8 Slutsatser och rekommendationer

8.1 Inledning

I detta kapitel lyfter vi fram de väsentligaste problemområdena. Därefter följer vår sammanfattande bedömning där vi besvarar den ställda revisionsfrågan. Avslutningsvis ger vi några rekommendationer.

8.2 Bedömning och slutsatser

Granskningen har till syfte att besvara följande fråga:

Arbetar Försäkringskassan, utifrån gängse normer, systematiskt med sin informationssäkerhet?

Granskningen visar på följande huvudsakliga brister.

8.2.1 Otillräcklig överblick över väsentligheter

Verksledning och verksamhetschefer på huvudkontoret saknar enligt vår bedömning tillräckligt stöd och hjälpmedel för att skapa en rättvisande och överblickbar bild över informationssäkerhetsriskerna i verksamhetens skilda delar – centralt, lokalt och inom IT-verksamheten[52]. Denna brist på möjligheter att överblicka riskerna medför enligt Riksrevisionens bedömning bl.a. svårigheter för myndighetsledningen att avgöra om beslutade säkerhetsåtgärder inom skilda verksamheter är i linje med av riksdag och regering beslutade normer eller av verksledningen fattade beslut. Ett sådant beslut utgör RFV:s beslut[53] från 2001 att längre avbrottstider än 24 timmar inte kan accepteras.

De ovan beskrivna bristerna vad gäller övergripande riskanalys och förmåga till översikt kan innebära att riskanalysen och prioritering av införande av kontrollåtgärder inte bygger på en tillräckligt god grund för att ge en god informationssäkerhet.

[52] Bl.a. enskilda försäkringsslag/produkter, utifrån geografisk belägenhet, med avseende på typ av risk, m.fl. aspekter.

[53] Detta beslut kvarstår oförändrat i den nya organisationen.

8.2.2 Riskanalysen är inte tillräckligt väl underbyggd och styrd

En brist är avsaknad av organisering och styrning av samlade analyser av informations- och IT-säkerhetsrisker för Försäkringskassan som helhet. Ingen har getts ett tydligt utpekat ansvar för att göra eller sammanställa en samlad riskanalys beträffande informationssäkerhet för Försäkringskassan. Med samlad riskanalys menas här en från verksamheterna underbyggd riskanalys.

Riskanalys är inte en väl integrerad del i systemutvecklingen, vilket kan leda till att säkerhetsrisker beaktas sent i utvecklingsprojekten eller i efterhand när systemen är driftsatta, vilket kan medföra dyrbara kompletterande säkerhetsåtgärder eller att risker inte uppmärksammas alls förrän incidenter inträffar.

Riskanalysarbetet har svaga kopplingar mellan central och lokal nivå, när det gäller styrning från central nivå och rapportering från länsnivå. Länsorganisationens arbete med riskanalyser varken styrs eller stöds från huvudkontoret. Det saknas uppföljning av kvaliteten hos analyserna som bedrivs i länen och utbildning i riskanalysmetoder, vilket bl.a. kan leda till brister i enhetlighet i synen på hur riskanalyser ska utföras och vilka skyddsåtgärder som ska prioriteras och genomföras.

En annan brist gäller riskanalysarbetets förutsättningar när det gäller omvärldsbevakning. Till exempel saknas en samlad bedömning av riskerna för brister i informationsutbytet mellan Försäkringskassan och andra myndigheter.

8.2.3 Nuvarande uppföljning av LIS och enskilda säkerhetsåtgärder ger inte svar på frågan om skyddet är tillräckligt

På en övergripande nivå saknar Försäkringskassan en sammanhållen åtgärdslista för säkerhetsåtgärder och uppföljning av dessa åtgärder. Försäkringskassan kan därför inte ge en samlad bild av hur de befintliga säkerhetsåtgärderna, och uppföljningen av dessa, tillsammans ger ett fullgott skydd. Den allvarliga incident som inträffade 2004 och som avsåg hantering av virusskydd är ett exempel på vad som kan inträffa när uppföljningen av säkerhetsåtgärder i LIS inte fungerar.

Uppföljningen av informationssäkerheten är endast till viss del organiserad i nuläget. Den uppföljning som finns avser till största delen enskilda säkerhetsåtgärder, t.ex. uppföljning av intern åtkomst (behörighetskontroll) av information, och inte om det LIS – delegationer, specialistenheter, metoder och stöd, arbete med riskanalyser, utbildning, uppföljningssystem etc. – som finns på plats fungerar på ett bra sätt.

En viktig brist avser kommunikationen i uppföljningsfrågor mellan länskontoren och central nivå. Det finns riktlinjer för uppföljande kommunika-

tion mellan länskontoren och huvudkontoret. Informationsutbytet kommer dock till stånd endast i mycket begränsad utsträckning.

Ledningens uppföljning av informationssäkerheten är i huvudsak reaktiv och händelsestyrd. De proaktiva inslagen – dvs. uppföljning av de beslutade åtgärderna och deras genomförande – är sparsamt förekommande. Verksledningen bedöms därför inte ha underlag för att göra en tillförlitlig uppföljning av gjorda delegationer.

Granskningen kan inte påvisa att Försäkringskassan systematiskt följer upp kvaliteten i riskanalyser och i använda modeller och metoder.

8.3 Sammanfattande bedömning

Den nya Försäkringskassan bildades den 1 januari 2005, vilket innebär att myndigheten nu existerat i drygt ett år. Många av de iakttagelser och brister vi noterat i denna granskning har inte uppstått under året, inte heller har det för den nya ledningen varit möjligt att upptäcka eller åtgärda alla brister under sitt första år. Flera av de iakttagna bristerna har sannolikt funnits under flera år. En del av bristerna kan sannolikt kopplas till svårigheterna att hantera det starka produktionstrycket och kraven på återkommande förändring av försäkringens innehåll. Vidare har vi noterat att flera förbättringar är planerade eller under införande, där flera av ovan beskrivna problem tas upp. Vi har dock i denna avrapportering valt att lyfta fram de brister vi funnit, oavsett om Försäkringskassan varit medveten om dem eller inte, eller om förbättringsåtgärder är planerade.

En annan omständighet som gällt i granskningen är dess inriktning och perspektiv. Vi har valt att lägga tyngdpunkten på myndighetsledningens styrning och kontroll för att säkerställa informationssäkerheten. Denna styrning och kontroll benämns samlat ledningssystem för informationssäkerhet (LIS). Denna avgränsning innebär bl.a. att faktiskt uppnådd säkerhet i enskilda system inte granskats.

Granskningen av Försäkringskassans ledningssystem för informationssäkerhet (LIS) visar att myndigheten infört flera av de delar av ledningssystemet som bör finnas enligt standarden SS-ISO/IEC 17799. Bland dessa finns behörighetskontrollsystem, fysiskt skydd för IT-systemen, säkerhetskopiering och ett stort antal andra skyddsåtgärder av administrativ och teknisk natur. Myndigheten har organiserat arbetet med informationssäkerhet samt utarbetat policydokument och riktlinjer för informationssäkerheten. Försäkringskassan har alltså flera av de delar som enligt standarden tillsammans utgör ett ledningssystem för informationssäkerhet.

Som framgått ovan är dock vissa delar av LIS mindre väl utvecklade. Dessa brister avser främst Försäkringskassans förmåga till överblick,

riskanalys och uppföljning. Bristerna medför att Försäkringskassans LIS sammantaget inte utgör en fullt ut lämpligt utformad och fungerande helhet. Det medför i sin tur att Försäkringskassans möjligheter minskar att samla de erfarenheter som gör systematisk förvaltning av LIS möjlig. Med förvaltning avses här det styrda förbättringsarbete som syftar till att förbättra LIS. Bristerna i LIS påverkar i sin tur möjligheterna att uppnå och vidmakthålla eftersträvad informationssäkerhet. Riksrevisionen konstaterar att Försäkringskassan under de två senaste åren har haft två händelser som medfört allvarliga konsekvenser för verksamheten, dels hanteringen av viruskyddet 2004, dels de problem som uppstod vid driftsättningen av FÄS/ÄHS 2005.

Svaret på den fråga som granskningen syftat till att besvara är därmed att Försäkringskassan inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

8.4 Rekommendationer

Försäkringskassan har under hösten 2005 utrett frågor avseende informationssäkerhet. Beslut är fattat den 27 januari 2006. Enligt Försäkringskassan skapas därmed ansvarsmässiga och organisatoriska förutsättningar för att Försäkringskassan ska kunna arbeta systematiskt med säkerhet utifrån gängse normer.

De väsentliga bristerna inom respektive del av LIS är ingående beskrivna i kapitlen 3 t.o.m. 7 och sammanfattade i avsnitt 8.2. I samma avsnitt – 8.2 – har de väsentligaste problemområdena angetts, dvs. överblick, riskanalys samt uppföljning. Försäkringskassan har i januari 2006 beslutat om en tydligare organisation för det fortsatta arbetet med informationssäkerhet. På så sätt har Försäkringskassan börjat åtgärda de brister i sitt LIS som tas upp i denna rapport.

Försäkringskassans ledning bör fortsätta att genomföra åtgärder för att komplettera sitt LIS i syfte att öka Försäkringskassans nytta av detta. En del av bristerna i LIS avser de funktioner – uppföljning och kontroll av LIS funktionssätt – som möjliggör ett systematiskt lärande beträffande LIS. Detta behövs för att Försäkringskassan ska kunna förbättra sitt LIS.

Vi vill särskilt framhålla betydelsen av att få en väl fungerande riskanalys som grund för väl underbyggda säkerhetsåtgärder. De beslutade säkerhetsåtgärderna behöver dokumenteras i en åtgärdsplan som sedan utgör grund för systematisk uppföljning av att åtgärder införs och fungerar som avsett. Riksrevisionen ser detta som en del av ett rapporterings- eller informationssystem som medger att verksledningen regelbundet och på ett specificerat sätt får tillgång till information från LIS skilda delar.

Bilaga 1 Komponenter i Försäkringskassans ledningssystem för informationssäkerhet (LIS)

I denna bilaga förtecknas de kontrollåtgärder som identifierats av Riksrevisionen under granskningen 2005[54]. Den baseras på uppgifter från dokument som Försäkringskassan överlämnat till Riksrevisionen samt från intervjuer med företrädare för Försäkringskassan.

Kontrollåtgärderna är sorterade efter de rubriker som används i rapporten:

- Ledningens kontrollmiljö
- Riskhantering
- Kontrollfunktioner och säkerhetsåtgärder
- Information och utbildning

Uppföljning, utvärdering och förvaltning av LIS

Ledningens kontrollmiljö

Övergripande reglering av betydelse för precisering av säkerhetsområden och strategi för säkerheten (inkl. informationssäkerhet).	Instruktion, Regleringsbrev, arbetsordning, säkerhetspolicy för Försäkringskassan, riktlinjer för allmän säkerhet, riktlinjer för krisberedskap, riktlinjer för informationssäkerhet samt beslut om Försäkringskassans säkerhetsorganisation.
Informationssäkerhetspolicy: definition, begrepp, områden och komponenter	Ett antal styrdokument finns för att styra arbetet med informationssäkerhet. Det centrala dokumentet är Riktlinjer för informationssäkerhet. Sammantaget motsvarar detta innehållet i en informationssäkerhetspolicy
Utgångspunkter för informationssäkerheten	Standarden ISO 17799, vilket bl.a. innebär att ett ledningssystem för informationssäkerhet ska finnas vid myndigheten. Vidare tillämpas Krisberedskapsmyndighetens Basnivå för IT-säkerhet (BITS).
Styrning av LIS	Ledningsgruppen som forum för diskussion och samråd i övergripande strategiska frågor. GD avgör. Återkommande samtal mellan GD och säkerhetschefen.
Övergripande ansvar för säkerheten	Generaldirektören[55]
Verksamhetsansvaret	Ansvar för säkerheten inkl. informationssäkerheten inom sin verksamhet Risk- och sårbarhetsanalyser Uppföljning och kontroll av rådande skyddsnivå samt hur säkerhetspolicyn efterlevs. Behörighetskontroller. Årliga ta fram handlingsplaner för säkerhet

[54] Försäkringskassans beslut den 27 januari 2006 ”Informtationssäkerhet gällande Organisation, Ansvar och Uppgifter” är inte beaktat.

[55] Detta ansvar har GD i första hand inför styrelsen som enligt instruktionen har ansvaret för verksamheten.

Ledningens kontrollmiljö

Allmänt ansvar	Det är var och ens ansvar att ta del av anvisningar och regler för säkerhet. Personalen ska kunna säkerhetsfrågorna. All personal ska vara medveten om hot och risker som rör informationssäkerheten.
Systemägare, system- och produktansvarig, IT-produktägare, systemförvaltare	Handlingsplaner för informationssäkerhetsarbetet (del av förvaltningsplan). Systemsäkerhetsplaner. Dokumentation av system. Säkerställa att skyddsåtgärder finns på plats. Driftgodkänner (inkl. säkerhet) Årlig uppföljning av förvaltningsplaner.
Säkerhetsfunktioner och -roller	Krisorganisation Säkerhetschef med säkerhetsstab, Informationssäkerhetschef med en informationssäkerhetsenhet IT-säkerhetschef med en IT-säkerhetsgrupp[56]. Säkerhetssamordnare som utses av divisionschefer och länsdirektörer att verka inom divisionen/länet. Lokala säkerhetsombud som utses av verksamhetsansvariga chefer på respektive lokaliseringsort. Incidentorganisation Samverkansformer såsom återkommande möten mellan säkerhetsfunktionerna, säkerhetskonferens, myndighetsgemensamma säkerhetsprojekt, säkerhetsråd, incidentråd samt WebbProcyRådet (om webbsidor). Stöd från bl.a. juridikstaben.
Säkerhetschefens ansvar	1 Ingår i ledningsgruppen fr.o.m. 2006, och kan svara rådgivande och stödjande gentemot verksamhetsansvarig chef. 2 Myndigheter ska genomföra risk- och sårbarhetsanalyser (årligen). Säkerhetschefen svarar för att denna analys sammanställs för hela FK. 3 Samordnar, beslutar om riktlinjer och rutiner, stödjer, ansvarar för åtgärder för fredstida krishantering och höjd beredskap, ansvarar för allmän säkerhet och incidenthantering. 4 Ansvarar för en sammanställd rapport som regelbundet tillställs verksledning
Informationssäkerhetschefens ansvar	1 Informationssäkerhetschefen ansvarar för uppföljning och kontroll inom verksamhetsområdet, samt för att följa upp utbildningsstatus och riskmedvetande inom myndigheten 2 Nya system och större systemändringar ska godkännas ur IT-säkerhetssynpunkt av produktägaren och informationssäkerhetschefen innan de tas i drift. 3 Som en del av verksamhetsplaneringen ska handlingsplaner utformas för informationssäkerhetsarbetet. Produktägaren gör detta inom ramen för förvaltningsplanen och i samverkan med informationssäkerhetschefen.

[56] Försäkringskassan tog den 27 januari 2006 beslut om ny säkerhetsorganisation för informationssäkerheten. Detta beslut har inte beaktats i granskningen.

Ledningens kontrollmiljö

II-säkerhetschefens ansvar	Det är varje verksamhetsansvarig chefs ansvar att säkerställa en fullgod IT-säkerhet, bl.a. genom att uppfylla gällande policy, riktlinjer och rutiner. IT-säkerhetschefen ska, på uppdrag av FK Datas chef, tillse att verksamheten lever upp till detta (vara informerad, övervaka – agera, bevaka, samverkan). IT-säkerhetschefens ansvar omfattar inte informationssäkerhetsarbete som rör annat än IT, t.ex. information på papper
IT-avdelningens ansvar	Att leverera förvaltnings-, service- och drifttjänster som svarar mot den övriga organisationens behov av informationssäkerhet.
Uppföljning	Incidentrapportering och incidenthantering

Riskhantering

Krav/utgångspunkter för riskanalyser	Riskanalys ska utföras enligt förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, krisberedskapsförordningen Riskanalys enligt förordningen (1995:1300) om myndigheters riskhantering I regleringsbrevet för 2005 understryks vikten av att Försäkringskassans kunder får ut sina ersättningar Interna regler finns för arbetet med analys av informationssäkerhetsrisker. Krav ställs på att regelbundna (årliga) risk- och sårbarhetsanalyser göras.
Förteckningar över informationstillgångar	Produktkarta, inventarieregister över IT-relaterad utrustning, systemkartor (år 2002).
Ansvarig för riskanalyser	GD kan ta initiativ till särskilda analyser.
	Säkerhetschefen genomför riskanalyser enligt förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, krisberedskapsförordningen samt enligt förordningen (1995:1300) om myndigheters riskhantering. Säkerhetschefen kan ta initiativ till särskilda analyser.
	Verksamhetsansvarig chef eller IT-produktägare ansvarar för att verksamheten belyses årligen i en risk- och sårbarhetsanalys. Verksamhetsansvariga chefer kan ta initiativ till särskilda analyser.
	System- och produktansvariga (dvs. systemägaren eller den som mottagit delegation från denne) genomför analys av säkerhetsbehov med hänsyn till systemens informationsinnehåll och verksamhetens krav.
	Informationssäkerhetschefen och IT-säkerhetschefen gör riskbedömningar inom sina sakområden
	Riskanalys på länsnivå görs i huvudsak av länssäkerhetssamordnarna. Länssamordnaren har träffar med länsdirektören. Beträffande incidenter överlämnas dock regelbundet statistik till länsdirektören
Säkerhetsklassning	Ska ske enligt de egna riktlinjerna för informationssäkerhet vid utveckling och modifiering av IT-system. Säkerhetsklassificering av verksamhetskritisk information.
Metod för riskanalys	Två metoder förekommer – SBA Check och SBA Scenario.
	Försäkringskassan medverkar i Krisberedskapsmyndighetens

Riskhantering

	samverkansgrupp för ekonomisk säkerhet. I denna grupp har man sedan 2003 analyserat riskerna i samhällets betalningssystem.
	Verksamhetsansvariga chefer inom Riksförsäkringsverket genomför en workshop med stöd från personal från Kammarkollegium med anledning av krav på riskanalys enligt förordningen (1995:1300) om myndigheters riskhantering
	Centralt analyser ad hoc på avgränsade områden
Underlag för riskanalys	Årliga analysrapporter per produkt/system (motsv) Årlig sammanställning från incidentrapporterna. Särskilda analyser för delområden Uppdateringar av risk och sårbarhet på produkt- och/eller IT-systemnivå
Incidentrapportering	Riktlinjerna finns med en detaljerad beskrivning
Överblick över alla risker	
Analys av åtgärder och åtgärdsplan	Skydd för respektive säkerhetsnivå beslutas av informationssäkerhetschefen och säkerhetschefen i samråd med produktägaren Behov av åtgärder analyseras efter incidenter Strategin för informationssäkerhet kommer till utryck genom verksamhetsplaneringen varje år.
Förteckning över beslutade och införda informationssäkerhetsåtgärder	

Kontrollfunktioner och säkerhetsåtgärder

Utgångspunkter för LIS	Standarden ISO 17799 i kombination med KBM:s vägledning BITS (baskrav för IT-säkerhet).
Omfattning av ledningssystem för informationssäkerhet - LIS	Övergripande policydokument och riktlinjer, ansvarsfördelning och organisation, krisorganisation, rutinbeskrivningar för vissa delar av säkerhetsarbetet samt ett flertal tekniska säkerhetsåtgärder som ingår i myndighetens IT-infrastruktur.
Organisation	En enhet har ett särskilt ansvar för informationssäkerhetsfrågor
Samlad dokumentation över införda säkerhetsåtgärder	
Kontrollplan/övergripande uppföljningsplan	Vissa uppföljningsaktiviteter finns: IT-avdelningen tar varje månad fram en s.k. ”Statusrapport leverans”.
Riktlinjer för IT-systemen/IT-produkter	Kontinuitetsplaner för IT-system, systemsäkerhetsplaner och systemförvaltningsplaner med beskrivningar av åtgärder som avser informationssäkerhet. Innan ett IT-system tas i drift ska systemet säkerhetsgodkännas av produktägare och informationssäkerhetschefen. Dokumentation med inslag av säkerhetsfrågor finns i Systemdokumentet Plan för affärsmässig förvaltning (förvaltningsplan) som omfattar bl.a. ett s.k. Service Level Agreement (SLA). Vidare finns dokumenten Driftdokumentation respektive Månadsrapport

Kontrollfunktioner och säkerhetsåtgärder

	Principer för att utforma informationssystem bl.a. så att krav på informationssäkerhet uppfylls.
Rutinbeskrivningar	Utveckling och förvaltning av IT-miljön, hantera produktionsändringar i IT-systemen, incidenthantering, hantering av personuppgifter, hantering av sekretessbelagda uppgifter, säker arbetsplats, in- och utloggning på arbetsplatser, arbete på resa, användning av Internet, distansarbete, virusskydd, användning av e-post i tjänsten, reparation/service/avveckling av IT-utrustning, kassering/utplåning av IT-medier som innehåller information samt skydd mot stöld av IT-utrustning
Tillgänglighet till dokument om informationssäkerhet	I Försäkringskassans intranät.
Tekniska säkerhetsåtgärder	Reservanläggning för IT-drift (alternativ datorhall), behörighetssystem, behörighetskontrollsystem, övervakningssystem, säkerhetskopiering av information, tester av incidentberedskapen, IT-stöd för rapportering och analys av incidenter, kryptering, anti-virus, brandväggar, digital arkivering, samt helpdesk

Information och utbildning

Systematisk utbildningsverksamhet och -process	
Utbildning	Finns, bl.a. e-baserad säkerhetsutbildning, som riktar sig till all personal. All personal ska genomgå utbildningen.
Information om säkerhetsregler	Skriftlig information finns, även på intranätet.
Uppföljningsplan för information och utbildning	
Verksamhetsansvarig	Uppföljning av användarnas riskmedvetande och kompetens att hantera informationssäkerhetsriskerna
	Att personalen får säkerhetsutbildning som är relevant för de aktuella arbetsuppgifterna
	Uppföljning och kontroll av hur säkerhetspolicyn efterlevs
	Uppföljning och kontroll av tilldelade behörigheter en gång per år
	Genomgång av säkerhetsfrågor med berörda personalgrupper är obligatorisk vid nyanställning, övergång till annan tjänst samt vid behörighetstilldelning, t.ex. för ett specifikt IT-system Tillse att anlitade konsulter får tillräcklig information och utbildning om informationssäkerhet
Allmänt ansvar	Det är vidare var och ens ansvar att ta del av anvisningar och regler för säkerhet. Alla ska känna till säkerhetspolicyn, riktlinjerna och rutiner för informationssäkerhet. Varje person ska följa de regler som anvisas av ledningen
Informationssäkerhetschefens och –enhetens ansvar	Följa upp utbildningsstatus och riskmedvetande inom myndigheten Sprida information och ta fram utbildning inom området.

Information och utbildning

Utbildning av chefer	
Utbildning av styrelsen	Styrelsen har fått information som rör vissa delar av säkerheten
Systematisk utbildning av säkerhetspersonal	

Uppföljning, utvärdering och förvaltning av LIS

Systematiska och regelbunden uppföljning av LIS som grund för vidareutveckling av LIS	
Uppföljningsansvar	Informationssäkerhetschefen och IT-säkerhetschefen har ett uppföljningsansvar enligt styrdokumenten
Organiserad uppföljning av LIS	
Uppföljning av delegationer	Verksledningen följer upp sina delegationer beträffande informationssäkerhet vid träffar 7– 8 gånger om året med säkerhetschefen
Avrapporteringsrutiner för uppföljning och utvärdering av LIS i sig	
Återkommande orienteringar om utvecklingen och händelser i omvärlden	
Systematiskt uppföljning av kvaliteten i riskanalyserna	
Kontroll av enskilda säkerhetsåtgärder	Penetrationstester, säkerhetsgranskning av IT-plattformarna och av rutiner för hantering av säkerhetsbrister i programvaror och hårdvara
Internrevisionen	Flera granskningar som berör skilda IT-system.
Uppföljning av personalens säkerhetsmedvetenhet	Det åligger också informationssäkerhetschefen och IT-säkerhetschefen att följa upp medvetenheten. Primäransvaret för uppföljning har de verksamhetsansvariga.
Övergripande plan för uppföljningen av säkerheten	
Övergripande granskning[57] av hur väl LIS fungerar	

[57] Frågorna kring ansvarsfördelning har dock utretts som underlag för beslutet i januari 2006.

Källförteckning

Lagstiftning

Tryckfrihetsförordning (1949:105)
Arkivlag (1990:782)
Personuppgiftslag (1998:204)
Sekretesslag (1980:100)
Skyddslag (1990:217)
Lag (2003:389) om elektronisk kommunikation

Förordningar

Arkivförordning (1991:446)
Förordning (1995:1300) om myndigheters riskhantering
Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap
Säkerhetsskyddsförordning (1996:633, 2000:888)
Datainspektionens allmänna råd: Säkerhet för personuppgifter (december 1999)
Personuppgiftsförordning (1998:1191)
Verksförordning (1995:1322)
Rikspolisstyrelsens föreskrifter om säkerhetsskydd (RPS FS 1996:9 FAP 244-1)

Texter från Internet

Mörkertalsundersökningen. Hämtad från http://www.pts.se/Archive/Documents/SE/Morkertalsundersokningen_2005.pdf
National Institute of Standards and Technology (NIST), special publications (SP):
Draft Special Publication 800-40 Version 2 – Creating a Patch and Vulnerability Management Program
Draft NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling
NIST DRAFT Special Publication 800-26, Revision 1: Guide for Information Security Program Assessments and System Reporting Form
Control Objectives for Information and related Technology (COBIT). Hämtat från ISACA
http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

Övrigt material

SS-ISO/IEC 17799, SS 627799. Ledningssystem för informationssäkerhet.

Krisberedskapsmyndigheten 2003. Krisberedskapsmyndighetens rekommendation 2003:2 Basnivå för IT-säkerhet (BITS).

National Institute of Standards and Technology (NIST), special publications (SP):

SP800-26 *Security Self-Assessment Guide for Information Technology Systems,*

SP800-27 Rev. A *Engineering Principles for Information Technology Security,*

SP800-30 *Risk Management Guide for Information Technology Systems,*

SP800-31 *Intrusion Detection Systems (IDS),*

SP800-33 *Underlying Technical Models for Information Technology Security,*

SP800-34 *Contingency Planning Guide for Information Technology Systems,*

SP800-35 *Guide to Information Technology Security Services,*

SP800-40 *Procedures for Handling Security Patches,*

SP800-41 *Guidelines on Firewalls and Firewall Policy,*

SP800-42 *Guideline on Network Security Testing,*

SP800-44 *Guidelines on Securing Public Web Servers,*

SP800-45 *Guidelines on Electronic Mail Security,*

SP800-46 *Security for Telecommuting and Broadband communications,*

SP800-47 *Security Guide for Interconnecting Information Technology Systems,*

SP800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices,

SP800-50 Building an Information Technology Security Awareness and Training Program,

SP800-55 Security Metrics Guide for Information Technology Systems,

SP800-60 Guide for Mapping Types of Information and Information Systems to Security Categories,

SP800-61 Computer Security Incident Handling Guide,

SP800-64 Security Considerations in the Information System Development Life Cycle,

SP800-65 Integrating Security into the Capital Planning and Investment Control Process.

Kommunikation avseende erfarenheter från andra nationella revisionsorgan, bl.a. GAO i USA, OAG i Kanada samt erfarenheter från den svenska bank- och försäkringssektorn.

Committee of Sponsoring Organizations of the Treadway Commission. Framework for assessing and developing an internal control structure (COSO).