RIKSREVISIONEN

Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten

ISBN 91 7086 059 9
RiR 2005:26
Tryck: Riksdagstryckeriet, Stockholm 2005

Till
Regeringen
Finansdepartementet

Datum 2005-11-17
Dnr 31-2004-1295

Statens pensionsverk interna styrning och kontroll av informationssäkerheten

Riksrevisionen har granskat Statens pensionsverk arbete med informationssäkerhet. Resultatet av granskningen redovisas i denna granskningspromemoria.

Företrädare för myndigheten har beretts tillfälle att faktagranska och lämna synpunkter på utkast till granskningspromemorian.

Promemorian överlämnas till regeringen i enlighet med 9§ lagen (2002:1022) om revision av statlig verksamhet m.m. Promemorian överlämnas samtidigt till Riksrevisionens styrelse.

Promemorian innehåller slutsatser och rekommendationer som avser Statens pensionsverk. Promemorian överlämnas därför även till Statens pensionsverk.

Revisionsdirektör *Dan Ljungberg* har beslutat i detta ärende. Revisionsdirektör *Björn Undall* har varit föredragande. Revisionsdirektör *Bengt EW Andersson*, revisionsdirektör, *Stefan Gollbo*, revisionsdirektör *Frank Lantz* och revisor *Fredrik Hallgren* har medverkat vid den slutliga handläggningen.

Dan Ljungberg

Björn Undall

För kännedom
Statens pensionsverk

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 och verksamhet. Det är både svårt och resurskrävande. Det är mot denna bakgrund som Riksrevisionen har ökat sina insatser i granskningen av informationssäkerhet inom staten. Denna granskning gäller Statens pensionsverks (SPV) arbete med informationssäkerhet.

Vad menas med informationssäkerhet?

Informationssäkerhet handlar om att rätt information ska finnas tillgänglig, att den inte ska kunna förvanskas eller vara möjlig att komma åt för obehöriga. Det ska också vara möjligt att spåra bakåt hur information använts och ändrats.

Riksrevisionen har i sin granskning utgått från en internationell standard för ledning av informationssäkerhetsarbete (SS-ISO/IEC 17799), den s.k LIS-standarden. Den täcker alla de områden som säkerhetsarbetet behöver omfatta, både det rent tekniska skyddet och det som handlar om att påverka de anställdas beteende.

Vad kan bristande informationssäkerhet leda till?

SPV hade 2004 en omslutning på 190 miljarder kronor. Det betalades ut 10 miljarder kronor utslaget på 280 000 utbetalningar per månad. Såväl beräkningen av pensionen och att utbetalningen går till rätt person, som beräkningen av myndigheternas premier är beroende av korrekta underlag. Misstag eller manipulation leder till märkbara konsekvenser både för enskilda och myndigheter då även små felaktigheter över åren kan summeras till betydande belopp.

Har SPV ett fungerande system för informationssäkerhet?

Både ja och nej. Vår bedömning är att de områden som SPV behöver arbeta med och utveckla är sådana som ofta är problematiska i säkerhetsarbete. Det finns styrdokument, men i kombination med omfattande delegering och högt produktionstryck prioriteras inte områden som samverkan, uppföljning och fortlöpande utbildning inom informationssäkerhetsområdet. Det starka förtroende för sina medarbetare som präglar SPV innebär också att riskanalysen, och därmed även skyddsåtgärderna, fokuserar på yttre hot. Även sekretessfrågorna fokuseras. Skyddet gentemot exempelvis interna hot blir då naturligt lägre prioriterat.

De delar av LIS (ledningssystemet för informationssäkerhet) som utgörs av styrdokument och i hög grad även tekniska skyddsåtgärder finns alltså till största delen på plats. Men, de delar av LIS som handlar om säkerhetsbeteende och samverkan mellan personer behöver utvecklas. Det senare är avgörande för att LIS ska göra avsedd nytta. Slutsatsen är att SPV inte fullt ut har lyckats åstadkomma de förutsättningar för god informationssäkerhet som de insatser och investeringar som gjorts i myndighetens LIS varit avsedda att åstadkomma.

Bristerna i LIS påverkar i sin tur möjligheterna att uppnå och vidmakthålla eftersträvad informationssäkerhet. Svaret på den fråga som granskningen syftat till att besvara är därmed att SPV inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

1 Inledning

1.1 Bakgrund, syfte och revisionsfrågor

Granskningen avser Statens pensionsverks (SPV) arbete med informationssäkerhet. Informationssäkerhet kan definieras i termerna:

- Tillgänglighet, att behöriga användare har tillgång till den information de är behöriga till i rätt tid och omfattning.
- Riktighet, att information inte obehörigt ändras eller modifieras.
- Sekretess, att endast behöriga användare kommer åt information.
- Spårbarhet, att kunna se vem som gjort vad och vid vilken tidpunkt.

Informationssäkerhet handlar med andra ord både om att rätt information ska finnas tillgänglig för att verksamheten ska kunna ge god service och om att informationen inte ska förvanskas eller komma obehöriga till del. Det ska också vara möjligt att i efterhand visa på vem som medverkat till att informationen använts eller ändrats i strid med myndighetens regler.

Informationssäkerheten är väsentlig i tiden därför att elektronisk förvaltning får insteg hos de flesta statliga myndigheter och allt större krav ställs på att sådana tjänster som tillhandahålls elektroniskt är säkra, inte minst för att medborgare och företagare ska ha förtroende för dessa tjänster. Med denna utveckling följer bl.a. att myndigheterna behöver se över och vid behov förstärka informationssäkerhet.

En rapport[1] från Sveriges IT-incidentcentrum, SITIC, som är en del av Post- och telestyrelsen visar att:

- 21 % av offentliga[2] organisationer har någon gång varit med om IT-säkerhetsincidenter som medfört att information eller systemkomponenter blivit åtkomliga 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.

[1] 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

[2] 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 ett system/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 virus, maskar, trojaner m.m.

SITIC:s undersökning visar att både hot och incidenter är verklighet för svenska myndigheter i dag.

Vilken praktisk betydelse skulle brister i SPV:s informationssäkerhet kunna få? Beräkningen av pensionsutbetalningar till pensionärerna, betalningen till rätt pensionär liksom beräkningen av myndigheternas premier och beräkningen av statens pensionsåtagande är alla beroende av informationens riktighet. Misstag eller manipulation kan därmed få svåra konsekvenser både för enskilda och myndigheter. Om exempelvis underlaget för beräkning av pension för en enskild pensionstagare är felaktig eller om beräkningen i sig görs på fel sätt, kan även små avvikelser över åren summeras till betydande belopp. Ett annat exempel är att utbetalningar görs till fel mottagare. Eftersom det är fråga om så stora belopp som SPV utbetalar, kan det finnas ett stort intresse för att genom medveten brottslig gärning t.ex. styra om en del av utbetalningarna till fel mottagare eller påverka intjänandeuppgifter, men självklart kan även misstag ligga bakom felaktiga utbetalningar.

Granskningen avser SPV:s arbete med informationssäkerhet. Under arbetets gång har Riksrevisionen valt att fokusera på säkerheten för de IT-relaterade informationstillgångarna. Säkerheten för manuella register, brev och liknande informationssamlingar har alltså inte blivit föremål för någon granskning. Det som Riksrevisionen därmed har granskat är därför det som brukar kallas IT-säkerhet. 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 legat på myndighetsledningens styrning och kontroll för att säkerställa säkerheten/skyddet av myndighetens IT-relaterade informationstillgångar, t.ex. systemdokumentation, informationsregister/databaser, programvaror och programlicenser. Denna styrning och kontroll benämns samlat för ledningssystem för informationssäkerhet (LIS). Denna avgränsning innebär bl.a. att faktiskt uppnådd säkerhet i

enskilda system inte granskats. God informationssäkerhet 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. Detta är bakgrunden till vårt val av LIS som fokus.

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

1.2 Bedömningskriterier

Riksrevisionen har i sitt sökande efter revisionsfrågans ”gängse normer” utgått från ett flertal normkällor[3]. Efter genomgången valdes standarden Ledningssystem för informationssäkerhet – Riktlinjer för ledning av informationssäkerhet (SS-ISO/IEC 17799 och SS 627799) som den dominerande utgångspunkten för Riksrevisionens granskningskriterier. Nämnda standard, den s.k. 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.”[4] Samtidigt utgör standarden ”en gemensam grund för i princip alla organisationer”[5].

För Riksrevisionens beslut att använda LIS-standarden har följande faktorer haft betydelse:

- LIS-standarden visar sig vid Riksrevisionens genomgång av de olika normkällorna vara den mest fullständiga. Med det menas att den täcker alla de områden – länkarna i kedjan – som säkerhetsarbetet behöver omfatta för att det ska leda till att eftersträvad säkerhet ska kunna uppnås.
- Det är vidare 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.

[3] 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.

[4] SS-ISO/IEC 17799 s. 10.

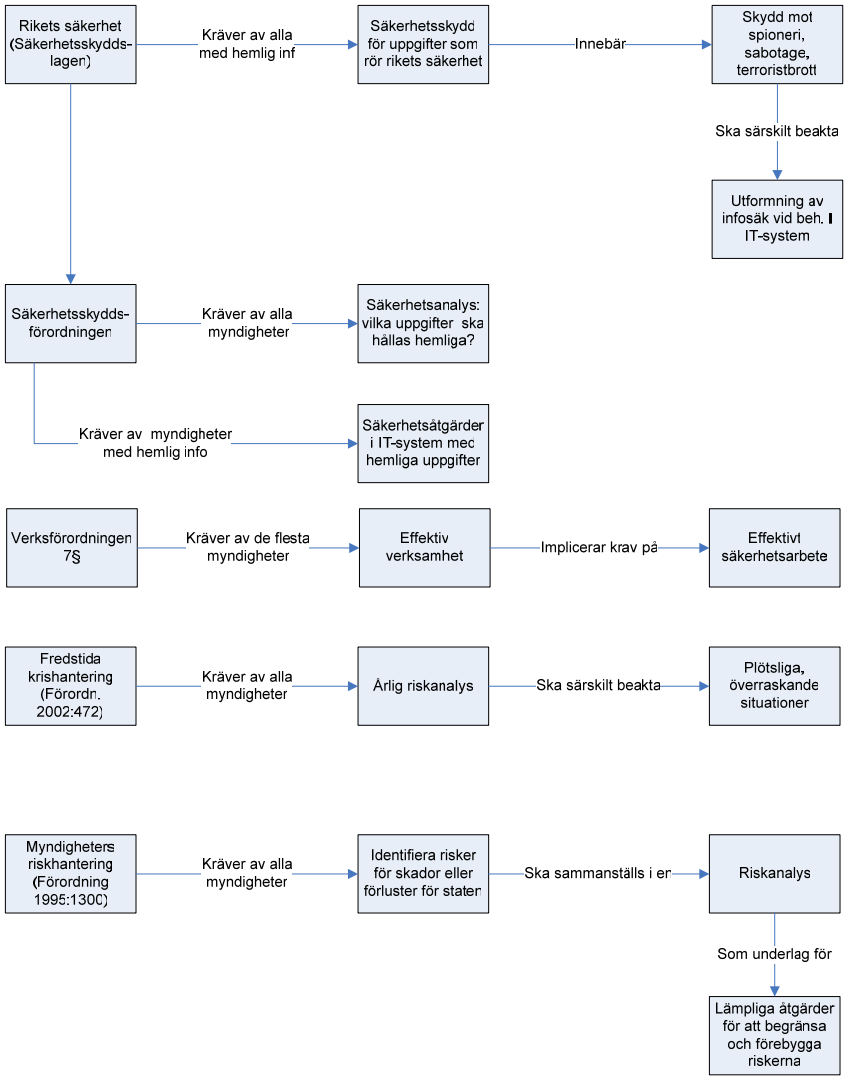
[5] SS-ISO/IEC 17799 s. 10.

- Standardens innehåll (riktlinjerna) har visats sig vara stabilt. Standarden har efter tio år nu uppdaterats beträffande sin disposition men den är innehållsligt intakt.

Riksrevisionen har således valt att använda LIS-standarden för att precisera de kriterier som bör gälla för att informationssäkerhetsarbetet ska anses bedrivas enligt gängse norm. På en övergripande nivå finns emellertid också krav på myndigheter i detta avseende formulerade i lagar och förordningar.

Lagar och förordningar som berör informationssäkerhet

Figur 1. Översikt över reglering av informationssäkerhet



Lagar och förordningar som berör informationssäkerhetsområdet beskrivs i grafen ovan[6]. De behandlar myndigheters riskhantering[7], åtgärder för fredstida krishantering[8] samt skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet[9].

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, säkerhetsskyddsförordning).

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 spionerі, 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 uppstå genom brister i informationssäkerheten för stora delar av den statliga informationen, och

---

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

[7] Förordning (1995:1300) om myndigheters riskhantering.

[8] Förordning (2002:472)om åtgärder för fredstida krishantering och höjd beredskap.

[9] Säkerhetsskyddslag (1996:627).

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. Riskhanteringsförordningen uppfattar därför Riksrevisionen 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 eller annan skada för staten.

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

1.2.1 LIS-standarden

Enligt Riksrevisionens tolkning av LIS-standarden ska åtgärder vidtas för skydd av all, enligt den enskilda myndighetens bedömning, *skyddsvärd information.* Det kan uppfattas innebära 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. Med detta krav följer bl.a. enligt Riksrevisionens bedömning att säkerheten för alla skyddsvärda informationstillgångar ska skötas i ett sammanhållet ledningssystem. 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. Granskningsprogrammet har behandlats i seminarier med Swedish Standards Institute (SiS), Krisberedskapsmyndigheten, Statskontoret och en säkerhetschef inom bank- och försäkringssektorn.

I granskningsprogrammet har således LIS-standarden använts som utgångspunkt för kriterier för bedömning av myndighetens säkerhetsarbete. Bedömningskriterierna avser myndighetens kontrollmiljö, riskanalys, kontrollfunktioner, information och utbildning samt uppföljning av och förvaltning. Bedömningskriterierna anges i inledning av kapitel 3-7.

1.3 Metoder och tillvägagångssätt i granskningen

Granskningen har genomförts på följande sätt:

- Myndigheten har först fått ett introduktionsbrev och en begäran att få ta del av myndighetens informationssäkerhetspolicy.
- Myndigheten har därefter fått besvara en webbenkät med frågor (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 av vilka av dess dokument som motsvarar Riksrevisionens beskrivningar och som tillsammans ger en rättvisande bild av myndighetens arbete med informationssäkerhet.
- Efter det att Riksrevisionen gått igenom dokumenten har företrädare för myndigheten blivit intervjuade[10] med stöd av granskningsprogrammets intervjufrågor. 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.
- Myndigheten har sedan faktagranskat utkast till revisionsrapport.

Med denna stegvisa insamling av information har det varit möjligt att sprida denna över en längre tidsperiod och därmed mindre belasta myndigheten. Det har samtidigt gjort det möjligt att fokusera insamlandet i efterföljande insamlingssteg utifrån resultaten av föregående steg.

[10] GD, cheferna för de två huvudavdelningarna, IT-chefen, IT-säkerhetschefen samt chefsjuristen.

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 SPV kommit i förhållande till vår tolkning av de krav som uttrycks i LIS-standarden.

I rapporten har redovisningen av granskningskriterier, iakttagelser och slutsatser strukturerats[11] enligt följande:

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

En beskrivning av Riksrevisionens bedömningskriterier för respektive komponent i modellen inleder kapitel 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. 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 SPV i myndighetens informationssäkerhetsarbete. 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.

[11] 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 SPV och informationssäkerheten

2.1 SPV:s verksamhet

SPV[12] har till uppgift att beräkna och utbetala tjänstepensioner och andra avtalsförmåner för anställda inom statsförvaltningen. SPV beräknar även pensionspremier för arbetsgivare och redovisar statens totala tjänstepensionsskuld.

Några fakta om SPV:s verksamhet:

- Omsättning: 272 miljoner kronor (år 2004)
- Antal pensionsutbetalningar: 280 000 utbetalningar per månad
- Pensionsutbetalningar i kr per månad: 10 miljarder kronor (år 2004)
- Balansomslutning: ca 190 miljarder kronor (år 2004)

De förordningar och föreskrifter som reglerar SPV:s verksamhet är:

- Förordning (1997:131) med instruktion för Statens pensionsverk
- Förordning (1997:908) om premier för statens avtalsförsäkringar
- Förordning (2002:869) om utbetalning av statliga tjänstepensions- och grupplivförmåner
- AgVFS 2000:1 A 1 Statens pensionsverks föreskrifter om lämnande av uppgifter till systemet för automatisk matrikelföring
- SAVFS 1990:3 A 1 om utbetalningen av personskadeersättning

Enheten Kund/pension (sammanslagning av de tidigare avdelningarna Staten och Uppdrag) är den i särklass största produktionsenheten inom SPV och svarar för administrationen av det som enligt de statliga pensionsavtalen leder fram till en pensionsutbetalning. Enheten innehåller flera sektioner såsom Kundsektionen och Sektion företag.

Den andra produktionsenheten Försäkringsenheten svarar för insamling av indata från arbetsgivarna angående anställningsförhållanden och löneutbetalningar och säkerställer korrekta uppgifter om detta i SPV:s databaser.

Utifrån dessa grunddata beräknas pensionsskuld och de premier som arbetsgivaren ska betala. Riktigheten i grunddata är väsentlig eftersom eventuella brister i denna således påverkar de premier som arbetsgivaren ska betala eller de belopp som utbetalas till pensionären. Detta speglas i SPV:s organisation (försäkringsenheten samt aktualiseringsverksamheten för pensionsavtalen). Arbetsgivarna har ansvaret för lämnade uppgifters

[12] I stora stycken hämtat från SPV:s webbplats.

riktighet. SPV har dock hittills ägnat betydande resurser åt att rätta felaktiga uppgifter i lönefilerna från arbetsgivarna. Detta har ändrats så att arbetsgivarna själva får utföra detta arbete, samtidigt som SPV ger dem IT-stöd som underlättar kontrollen.

SPV har ett outsourcingavtal beträffande hela sin stordatordrift.

2.2 Informationstillgångarna och SPV:s bedömning av deras säkerhet

Inslaget av IT-stöd i SPV:s processer är betydande och SPV är starkt IT-beroende.

Det ställs stora krav på att den information som finns i SPV:s informationssystem är säkerställd. Med detta menas att informationens riktighet, tillgänglighet och sekretess är skyddad. Kraven på kontinuitet i verksamheten är också stora.

Enligt Riksrevisionens enkät till myndigheten betraktar SPV informationssäkerhet som en viktig ledningsfråga.

Ett flertal faktorer i myndighetens verksamhet påverkar SPV:s bedömning av informationssäkerhetens betydelse i verksamheten. SPV framhåller i sitt svar på Riksrevisionens webbenkät att omfattningen av IT-beroendet, omfattningen av e-tjänster och exponeringen på Internet, vikten av kontinuitet och volymen incidenter är särskilt betydelsefulla faktorer för utformningen av arbetet med informations-/IT-säkerhet.

Sammantaget anser SPV enligt enkätsvaret att myndigheten har en informationssäkerhet som är tillräcklig.

SPV har upprättat en informationssäkerhetspolicy av vilken det framgår på ett övergripande plan målsättning, definition och ansvar för informationssäkerheten. Policyn är beslutad av GD. Av policyn framgår att SPV har valt en starkt decentraliserad organisering av sitt informationssäkerhetsarbete. GD är övergripande ansvarig, säkerhetschefen är ansvarig för att säkerheten upprätthålls och för samordning av säkerheten, vidare framgår att ansvaret för informationssäkerheten följer verksamhetsansvaret. Utöver informationssäkerhetspolicyn finns ett antal beslutsdokument som reglerar olika frågor rörande informationssäkerheten.

Enhetscheferna är systemägare. Bland systemägarens ansvar ingår ansvaret för skyddet av systemen. IT-chefen är systemägare för IT-infrastrukturen[13] och ansvarar för alla de tekniska skyddsåtgärder som vidtagits (behörighetskontrollsystem, virusskydd m.m.).

[13] Med IT-infrastruktur avser SPV det gemensamma generella tekniska IT-stöd, i form av program- och maskinvaror, som verksamheten ges tillgång till.

SPV har under många år utvecklat en mängd IT-system[14] som stöd för förvaltningen av de statliga pensionsavtalen. Några av dessa är stora och innehåller ett flertal stora databaser såsom GRU och SKULD. De flesta stora systemen har Försäkringsenheten som systemägare. Under 2004 driftsattes IT-stödet för det nya pensionsavtalet PA03 som utvecklats i projektet Nypon. Detta innebär bl.a. att SPV under flera år kommer att ha dubbla system för att klara hanteringen av samtliga pensionsavtal. År 2004 startade vidare en s.k. pensionsportal på Internet som utvecklats av Försäkringskassan med deltagande från bl.a. SPV. Pensionsportalen hämtar in information om respektive medborgares pensionskapital från alla aktuella pensionsinstitut och gör sedan en pensionsprognos för individen.

[14] De viktigaste är: Förmåner, Premier, Skuld, SPÅ, P-skuld, Utbetalningsprognos, IÅP, Kollekt/Mareg/ERF, Utbetalning//Beviljanden, Fam/Diabas.

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, 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

SPV har en **informationssäkerhetspolicy** i vilken bl.a. innebörden av informationssäkerhetsbegreppet definieras i enlighet med LIS-standarden och hur ansvaret för informationssäkerheten fördelas inom SPV.

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

Generaldirektören har delegerat ansvaret för informationssäkerhet till enhetscheferna som tillika är systemägare inom sina respektive enheter. Det har skapats en mängd andra roller som på skilda sätt berör informationssäkerhetsarbetet. Vid SPV finns en säkerhetschef vars ansvar är tillsyn och samordning av arbetet med informationssäkerhet. Utöver dessa ansvariga finns ett antal funktioner/roller som ska stödja arbetet med informationssäkerhet, t.ex. säkerhetsråd, säkerhetssamordnare, verksjurist, systemägarrepresentant och verksamhetsbeställare. De formella organisatoriska förutsättningarna har alltså preciserats.

Vid våra intervjuer har det framkommit att det emellertid råder olika uppfattningar om de olika rollernas ansvar och uppgifter. Sådan oklarhet råder beträffande verksamhetsbeställarna, systemägarrepresentanterna och säkerhetssamordnarna. Flera intervjuade känner för övrigt inte till att den sistnämnda rollen finns inrättad. Rollen som säkerhetssamordnare finns inskriven i informationssäkerhetspolicyn.

Av intervjuerna framgår att samverkan mellan enhetschefer, säkerhetschef och IT-chef är mindre väl utvecklad, trots att detta är nyckelrollerna vid sidan av GD i informationssäkerhetsarbetet. Flera av de intervjuade beskriver sitt arbete med informationssäkerhetsfrågor som något som sker i delegerad form inom den egna enheten – utan större behov av samverkan med omgivningen.

En annan förutsättning i detta sammanhang är att det finns en gemensam syn på vad som ska ingå i begreppet informationssäkerhet. Av intervjuerna framgår emellertid att större delen av de intervjuade cheferna i sina resonemang och analyser beträffande informationssäkerhet i stor utsträckning enbart fokuserar på sekretessriskerna och risk för obehörig åtkomst av sekretessbelagd information i systemen.

Verksledningens **engagemang** i informationssäkerhetsfrågor framgår på flera skilda sätt. SPV:s ledningsgrupp[16] samråder om och samordnar frågor av betydelse för verksamheten. Granskningen visar att incidentrapportering är den fråga som rör informationssäkerhet som är regelbundet återkommande (varje kvartal) på ledningsgruppens agenda. I övrigt finns ingen regelbundet återkommande rapportering som avser informationssäkerheten. Frågor avseende informationssäkerhet har som redan nämnts delegerats till verksamhetscheferna i linjen. Detta utgör i sig inget problem, men förutsätter att delegationen följs upp på ett ändamålsenligt sätt av GD och/eller ledningsgruppen. Detta sker således i mindre utsträckning. Det är vidare oklart på vilket sätt enhetscheferna följer upp sin vidaredelegation till sektionschefer. Riksrevisionen återkommer till frågan i kapitel 5.

[16] SPV:s ledningsgrupp består av: GD, ekonomichef, personalchef, chefsjurist, IT-chef, informationsdirektör, enhetschef Kund & Pension, enhetschef Försäkring samt pensionschef.

Ledningen gav under hösten 2003 ett konsultföretag i uppdrag att göra en riskanalys av IT-miljön. Denna resulterade i en omfattande rapport under november samma år. Flera iakttagelser och rekommendationer i denna är inte begränsade till att endast avse IT-miljön utan avser ledningens styrning av informationssäkerhetsarbetet. Riksrevisionen tar inte ställning till riktigheten i rapportens innehåll, men de frågor som tas upp borde ha lett till en grundlig analys och ställningstagande från bl.a. alla enhetschefer. Rapporten visar sig dock vara okänd för flertalet chefer som intervjuats och den har inte behandlats i ledningsgruppen såsom ansvarig för informationssäkerheten och LIS. Riksrevisionen tillskriver även denna iakttagelse engagemangskriteriet.

Beträffande verksledningens **förtrogenhet** med informationssäkerhetsarbetets ledningsfrågor kan konstateras att någon gemensam utbildning kring dessa frågor inte ägt rum. Granskningen visar vidare att det finns olika uppfattningar bland intervjuade chefer om informationssäkerheten är god eller inte. En del chefer anser att säkerheten är god med utgångspunkt i det lilla antalet incidenter som har kommit till deras kännedom. Emot detta talar en del som framkommer under intervjuerna[17] och som pekar på att det finns indikationer på förhöjd risk för brister i informationssäkerheten. Denna uppfattning styrks också av den tidigare nämnda konsultrapporten. Några av de intervjuade cheferna anser vidare att SPV inte är något intressant mål för en angripare eftersom myndigheten, enligt dem, hanterar relativt okänslig/ointressant information i angriparens tänkta perspektiv. När Riksrevisionen under intervjuerna beskriver några scenarier (liknande de som kort beskrivits i avsnittet 1.1) som visar på motsatsen överges denna ståndpunkt.

3.3 Bedömning

Den enligt Riksrevisionens bedömning viktigaste effekten av en god kontrollmiljö är att ledningen lyckats skapa välfungerande kommunikation och samverkan mellan skilda roller i informationssäkerhetsarbetet. LIS är ett system vars delar måste samverka för att tillsammans kunna leverera avsett resultat. Samverkan och kommunikation beträffande informationssäkerhetsarbetet påverkas av de förhållanden som redovisats ovan.

De ovan beskrivna oklarheterna om vad informationssäkerhet i praktiken omfattar medför risk att riskanalys, säkerhetsåtgärder och uppföljning av informationssäkerheten får en alltför snäv omfattning. Dessa risker kommer att beröras i påföljande kapitel. Här konstateras att den korrekta innebörden

[17] Bl.a. att information och utbildning för personalen, inte minst för chefer, inte är tillräcklig, att systemägare inte kontrollerar hur väl säkerhetsåtgärderna faktiskt fungerar.

lagts fast i SPV:s informationssäkerhetspolicy och att policyn följaktligen inte kommunicerats på ett effektivt sätt inom SPV.

Systemägarna har hos SPV fått en nyckelroll i arbetet med informationssäkerheten. Verksledningen har dock inte infört sådana kontrollfunktioner att det till ledningen kan kommuniceras en samlad bild av hur väl arbetet med informationssäkerhet i praktiken utförs i linjen och om systemägarna med stöd av säkerhetschefen och övrig organisering som beskrivits ovan förmår verka för att kraven på informationssäkerhet uppfylls.

Den konsultrapport som togs fram i slutet av 2003 borde enligt Riksrevisionens mening ha motiverat ledningen att kommunicera den inom informationssäkerhetsorganisationen för att på ett strukturerat sätt ta ställning till rapportens iakttagelser och förslag till vidare åtgärder, för att sedan användas av ledningen i bl.a. uppföljningssyfte. Inget av detta har skett. Riksrevisionen gör ingen bedömning av kvaliteten i konsulternas arbete, utan tar upp behandlingen av denna rapport som ett exempel på hur kommunikation och samverkan sker inom SPV beträffande informationssäkerhetsfrågor.

Riksrevisionen bedömer sammantaget att ledningens kontrollmiljö avseende informationssäkerhet har brister som hindrar kommunikation och samverkan mellan skilda roller i informationssäkerhetsarbetet.

4 Riskanalys

4.1 Bedömningskriterier

Riskanalys är en viktig förutsättning för och del av myndighetens riskhantering. 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[18] 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 – **informationsklassning** – med hänsyn till verksamhetens krav på säkerhet så att en prioritering av åtgärder kan göras.

Riskanalysen bör utföras med hjälp av beslutade och dokumenterade **metoder**[19]. Riskanalys bör årligen, och däremellan vid behov, uppdateras.

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

Det bör finnas en tydlig och uppföljningsbar **åtgärdsplan** som förtecknar beslutade åtgärder[20] för att möta de risker som framkommit i analysen t.ex. avbrottsplanering och förstärkning av skyddsåtgärder. Planen bör beskriva när åtgärderna ska vara genomförda och vem som ansvarar för deras genomförande.

I riskhanteringsarbetet ingår att ta hänsyn till **incidenter** för att på så sätt kunna skapa förutsättningar för att 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.

---

[18] 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.

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

[20] Dvs..åtgärder och kontroller som vidtas för att uppfylla specificerade säkerhetskrav som avser en viss informationstillgång. Skyddsåtgärderna omfattar bl.a. organisation och ansvar, administrativa rutiner, personalsäkerhet, fysiskt skydd, driftrutiner samt utrustnings- och programvarubaserade funktioner. Åtgärderna kan även indelas i förebyggande skydd, detekterande skydd och återställningsrutiner.

4.2 Iakttagelser

Det finns ingen samlad **förteckning** över SPV:s informationstillgångar, ej heller över databaser och de i dessa ingående informationsslagen.

Föreskrifter finns angående **informationsklassificering**. En informationsklassning har också gjorts inom SPV. Den avsåg informationen i det system som utvecklats i projekt Nypon. Informationstillgångar som är äldre och som t.ex. hör ihop med PA91 är inte klassade. Sammantaget är därför en stor del av tillgångarna inte klassade.

SPV lämnar årligen en riskanalys till departementet. Analysnivån i denna varierar från år till år. År 2003 gjordes en övergripande riskanalys som avsåg SPV. Analysen skulle tillgodose alla de tre förordningarnas[21] krav om riskanalys och lämnades till departementet. Den föranledde inga frågor eller andra vidare kontakter med Regeringskansliet. Analysen gjordes vid ett möte i ledningsgruppen som främst fokuserade risker för olyckor såsom brand och liknande. Arbetet med riskanalysen utförs dock inte i en process med beslutade och dokumenterade **metoder**. Säkerhetschefen ansvarar för analysen, och det är också han som initierar uppdatering av dokumentet.

Det framgår av SPV:s informationssäkerhetspolicy att det som (i enlighet med t.ex. LIS-standarden[22]) avses med informationssäkerhetsbegreppet är tillgänglighet, riktighet, sekretess och spårbarhet. Som nämnts ovan är SPV:s analyser av informationssäkerhet i stor utsträckning fokuserade på sekretessriskerna och risk för obehörig åtkomst av sekretessbelagd information i systemen. Detta kan medföra att andra **väsentliga risker** än sekretessrisker – exempelvis att någon, inom eller utanför myndigheten, skulle manipulera riktigheten i uppgifter som ligger till grund för framtida pensionsutbetalningar – underskattas eller inte tillräckligt uppmärksammas. Uppfattningen att både interna och externa aktörer måste bedömas ha ett potentiellt intresse av att påverka parametrarna som styr beräkning av egna eller närståendes pensionsbelopp delas inte av alla intervjuade. Att riktigheten därigenom skulle behöva betraktas som hotad både internt och externt har heller inte framgått i myndighetens riskanalyser. Detta till trots finns det flera säkerhetsåtgärder som försvårar genomförandet av sådana hot.

Fokus kring säkerhet ligger på behörighetstilldelning, tekniska lösningar och IT-infrastruktur. Fysiska risker för datormiljön har uppmärksammats och en ny datorhall ska upprättas där brand- och stöldskydd är prioriterat.

De säkerhetsåtgärder som planeras sammanförs inte i en tydlig och enkelt uppföljningsbar **åtgärdsplan**. Åtgärderna finns spridda i andra dokument, bl. a. systemförvaltningsplaner.

---

[21] SFS 1995:1300, SFS 1996:633 samt SFS 2002:472.

[22] SS-ISO/IEC 17799, SS 627799.

SPV har en rutin för rapportering av **incidenter**[23] där det anges varför rapportering ska ske och exempel på vad en incident är. En mall finns att fylla i som ska sändas till säkerhetschefen med kopia till enhetschef. Av intervjuer framgår dock att incidenter inte rapporteras in i den omfattning som de faktiskt förekommer. De incidenter som rapporteras är till väsentlig del av karaktären driftsstopp och annat som gör att personalens arbetsmöjligheter påverkas. Det fåtal incidenter av karaktären otillbörlig informationsåtkomst som konstaterats tycks inte ha fångats upp av myndighetens interna kontrollsystem, utan framkommit på annat sätt, bl.a. genom att anmälan från berörda personer inkommit till SPV.

4.3 Bedömning

SPV:s verksamhet är omfattande och komplex. Samma förhållande gäller myndighetens informationstillgångar. Det är därför en brist att möjligheterna att med hjälp av en förteckning eller databas skapa överblick över informationstillgångarna, de säkerhetskrav som gäller varje enskild tillgång samt de säkerhetsåtgärder som införts för deras skydd inte tillvaratagits. Detta påverkar möjligheterna till systematisk riskhantering negativt.

Samma effekt får de ovan beskrivna bristerna i riskanalysarbetets metoder samt frånvaron av en övergripande åtgärdsplan. Utan att ta ställning till den tidigare nämnda konsultrapportens kvalitet hade det varit naturligt att verksledningen gemensamt tagit ställning till vilka åtgärder som skulle genomföras, när de ska vara genomförda och vem som ansvarar för genomförandet.

Fokuseringen på sekretessrisken ökar risken för att övriga kontrollmål, integritet och riktighet, inte tilldelas den uppmärksamhet de kräver.

Sammantaget bedömer Riksrevisionen att SPV:s riskanalys har påtagliga brister.

[23] SPV, Rutiner för rapportering av incidenter dnr 2003-318-571.

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 policier och regler med avseende på 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[24]:

- 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[25],
- process för säkerhetskopiering av all verksamhetskritisk information.
- process för styrning av utveckling/förändringar i IT-miljö, IT-system och bemanning,

[24] 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.

[25] 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[26] 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**[27] 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

Granskningen visar att SPV har ett **LIS med dokumenterade och beslutade komponenter**.

LIS **omfattar** policydokument och ett flertal tekniska säkerhetsåtgärder som ingår i myndighetens IT-infrastruktur (behörighetskontrollsystem, virusskydd, brandväggar m.m.) för att skydda informationstillgångarna. Dock saknas flera av de komponenter som enligt standarden bör ingå i LIS, såsom kontinuitetsplan för den lokala IT-miljön, samlad åtgärdsplan, distansarbetspolicy, dokumenterad process för utbildning och information, återkommande uppföljning av användarnas riskmedvetande och kompetens att hantera informationssäkerhetsriskerna samt processer för återkommande uppföljning och förvaltning av LIS.

Myndigheten har ett uttalat förhållningssätt till distansarbete men detta fokuserar på det arbetsrättsliga perspektivet och bortser från säkerhetsaspekterna. Enligt SPV bedrivs inget distansarbete och därför krävs ingen distansarbetspolicy.

Ledningens uppföljning av SPV:s informationssäkerhet har brister när det gäller personalens efterlevnad av myndighetens regelverk som avser informationssäkerhet. Ett exempel är att det i dokumentet ”Riktlinjer för behörighetstilldelning” anges att verksamhetsansvarig ska vidta särskilda

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

[27] 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.

skyddsåtgärder, såsom regelbunden uppföljning av loggar, i de fall transaktioner hanteras som är känsliga ur säkerhetssynpunkt. Dessa särskilda skyddsåtgärder följs inte upp så att det tydligt framgår att de faktiskt utförs.

Systemägaransvaret har som tidigare nämnts lagts på enhetscheferna. Dessa hanterar denna delegation på olika sätt med avseende på vidaredelegering av arbetsuppgifter m.m. Systemägaren har enligt bl.a. informationssäkerhetspolicyn ett omfattande ansvar för informationssäkerhetsfrågor, men i de fall rollen vidaredelegerats görs inte uppföljning av hur väl det delegerade ansvaret praktiskt hanterats.

SPV har inte prövat sin informationssäkerhet genom intrångsförsök och det har inte heller gjorts något praktiskt test av att myndighetens kontinuitetsplanering fungerar som avsett.

Det finns brister i de tekniska skyddsåtgärderna. SPV har systembehörigheter och inte informationsbehörigheter. En användare kan därmed t.ex. söka på personer som inte är föremål för användarens handläggning.

Kopplingen mellan informationssäkerhetspolicyn och underliggande dokument anses inte vara tillräckligt tydlig av intervjuad personal[28].

Riksrevisionen har kunnat iaktta brister i **införandet** av LIS. Informationssäkerhetspolicyn har inte kommunicerats på ett fullgott sätt. Beslutade delegationer har inte alltid dokumenterats. Riskanalysprocessens metoder har inte beslutats och dokumenterats. Utbildningsprocessen omfattar inte stora personalgrupper, vilket beskrivs i följande kapitel om information och utbildning.

Bland annat de i avsnitt 4.2 påpekade bristerna i riskanalys och incidenthantering innebär att delar av SPV:s LIS inte utformats utifrån **best practice.**

5.3 Bedömning

Flertalet av de väsentliga styrdokument som utgör grunden för ett LIS finns vid SPV. De dokument som saknas avser främst distansarbetspolicy, kontinuitetsplan för lokal IT-miljö, samlad åtgärdsplan samt uppföljnings- och informationsaktiviteter. SPV:s utgångspunkt när det gäller distansarbetspolicy stöder sig på arbetsmiljölagstiftningens definition av begreppet distansarbete, dvs. arbete utförs under längre perioder från exempelvis hemmet. Enligt Riksrevisionens uppfattning är denna syn på distansarbete för begränsad ur informationssäkerhetssynpunkt eftersom all form av åtkomst från personalens sida till myndighetens informationsresurser från extern plats, såsom hemmet, Internetcaféer etc., i princip innebär samma

[28] Exempel på områden där förtydliganden efterfrågats är hur resultatet av SPV:s informationsklassificering ska implementeras praktiskt i behörighetshanteringen.

risk. Sådant arbete bedrivs bl.a. av myndighetens chefer med hjälp av utrustning som tillhandahålls av SPV. I LIS omfattning saknas alltså flera komponenter.

Riskanalys och den därtill knutna incidentrapporteringen är nyckelprocesser i informationssäkerhetsarbetet. Riksrevisionen bedömer att dessa inte är utformade utifrån ”best practice” på området. Rutinerna för styrning och uppföljning av informationssäkerhetsarbetet kan också utvecklas.

Sammantaget bedömer Riksrevisionen att konstaterade svagheter i kontrollfunktionernas omfattning och utformning (best practice) medför ökad risk för brister i informationssäkerheten.

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.

Det bör finnas en **process** för systematisk och återkommande information och utbildning beträffande informationssäkerhet till **berörda personalgrupper**[29]. 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. För cheferna ska det vidare finnas välfungerande **informations-/rapporteringsrutiner** som ger erforderligt underlag för ledningsarbetet som avser informationskvalitet.

6.2 Iakttagelser

Det finns ingen systematisk **process** för utbildning av olika **personalgrupper**, inklusive chefer. Nyanställda får genomgå en kurs som behandlar behörigheter, dataintrång och hantering av sekretessbelagd information. Någon systematisk information och utbildning ges däremot inte därefter. På eget initiativ kan personalen begära att få förkovra sig i avgränsade delar av informationssäkerhetsområdet, t.ex. offentlighetsprincipen. I de intervjuer Riksrevisionen har genomfört har det framgått att det finns brister i ledningens kunskaper om informationssäkerhetsarbetets olika delar och hur de hänger samman. Någon gemensam utbildning inom ledningsgruppen för att avhjälpa detta har inte genomförts. Säkerhetschefen har gått runt på enheterna och informerat om säkerhetsfrågor. Det är dock ingen återkommande aktivitet. Det finns ingen beslutad systematisk **process** som täcker

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

utbildning och information till SPV:s skilda behovsgrupper med undantag för nyanställda. En stor del av personalen får alltså inte återkommande utbildning och information i informationssäkerhet.

6.3 Bedömning

De nämnda iakttagelserna som avser SPV:s process för utbildning leder till Riksrevisionens bedömning att SPV inte hanterar behovet av fortlöpande information och utbildning inom informationssäkerhetsområdet på ett strukturerat sätt eller i övrigt på det sätt som LIS förutsätter. Ledningen har alltså inte infört tillräckliga funktioner för att försäkra sig om att personalen får tillräckliga kunskaper om informationssäkerhet och följer de regler som finns. Detta ökar risken för brister i LIS funktion och därmed i informationssäkerheten.

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.**

Verksledningen bör också följa upp beslutade **delegationer.**

Uppföljningen bör ge svar på om följande **väsentliga delar** av LIS fungerar som avsett:

- Riskanalysprocessen,
- åtgärdsplanering och genomförande av planerna,
- Incidentrapporteringen,
- Kontinuitetsplaneringen,
- den interna kontrollen beträffande information och utbildning angående informationssäkerhet,
- 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.),
- den interna kontrollen av efterlevnaden av det regelverk för upprätthållande av informationssäkerhet som grundas på informationssäkerhetspolicy, Internetpolicy, e-postpolicy, distansarbetspolicy m.fl.
- den faktiskt uppnådda informationssäkerheten systematiskt prövas och uppfyller säkerhetskraven,

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

Systematisk och regelbunden uppföljning av SPV:s informationssäkerhetsarbete tillämpas i liten omfattning inom SPV. Det sker exempelvis ingen uppföljning av personalens/IT-användarnas informations- och utbildningsbehov. Cheferna utgår från att personalen vet vad de får och inte får göra men hur kunskaperna faktiskt är i detta avseende har inte följts upp.

Uppföljning saknas beträffande flera av de i LIS ingående **väsentliga delarna,** såsom riskanalysprocessen, gjorda delegationer, information och utbildning samt den faktiskt uppnådda informationssäkerheten.

En förutsättning för verksledningens uppföljning är att det finns tydliga krav **dokumenterade** på enhetschefernas informationssäkerhetsarbete – utöver det som står att läsa i informationssäkerhetspolicyn. Som en konsekvens har ledningsgruppen inte heller etablerat någon tydlig uppfattning om hur uppföljning av **delegationen** till linjecheferna beträffande informationssäkerheten ska ske, främst hur verksledningen avser kontrollera hur enhetscheferna har kontrollerat/följt upp sina delegationer till sektionschefer och till andra roller.

Riksrevisionen har inte heller kunnat finna en dokumenterad process för **förvaltning och utveckling** av SPV:s LIS. Detta arbete faller på säkerhetschefen, men det finns inga tydliga ställningstaganden från verksledningens sida beträffande utvecklingen av LIS. Säkerhetschefen har heller ingen budget för detta ändamål.

7.3 Bedömning

Ett ändamålsenligt LIS består av en kedja av samverkande delar. De brister i systematik i uppföljningen av väsentliga delars funktionssätt som påpekats ovan försämrar verksledningens möjligheter till överblick av säkerhetsarbetets ändamålsenlighet och försämrar möjligheterna att förvalta och utveckla myndighetens LIS. Konsekvenserna av bristande uppföljning blir därigenom många och komplexa. Bristande uppföljning av exempelvis personalens kunskaper om regelverket för informationssäkerhet och dess tillämpning innebär förhöjd risk för brister i informationssäkerheten eftersom kunskapsbristen inte kommer att beaktas i myndighetens riskanalyser. Riskanalysen (delen sårbarhetsanalys) utgår därmed inte från en samlad bild av det faktiska sårbarhetsläget och ledningens bild av det säkerhetsläget blir osäker.

Riksrevisionens slutsats är att bristerna i uppföljning minskar ledningens möjligheter till rationella beslut om förbättringar i säkerheten och om utvecklingen av LIS.

8 Slutsatser och rekommendationer

8.1 Inledande lägesbeskrivning

Granskningen av Statens pensionsverks (SPV) ledningssystem för informationssäkerhet (LIS) visar att myndigheten infört flera av de delar av ledningssystemet som bör finnas enligt standarden SS-ISO/IEC 17799[30]. Bland dessa finns exempelvis behörighetskontrollsystem, eget skalskydd och rutiner för säkerhetskopiering. Myndigheten har också utarbetat policier samt riktlinjer för organisering av ansvaret för olika frågor som avser informationssäkerheten.

Riksrevisionen konstaterar att SPV under senare tid inte har haft – eller inte upptäckt – några allvarliga säkerhetsincidenter.

8.2 Bedömning och slutsatser

Granskningen har till syfte att besvara följande fråga:

Arbetar Statens pensionsverk, utifrån gängse normer, systematiskt med sin informationssäkerhet?

Granskningen visar på följande huvudsakliga brister.

8.2.1 Brister i samverkan i informationssäkerhetsarbetet

Den omfattande delegeringen i kombination med många inrättade befattningstyper inom informationssäkerhetsarbetet ställer stora krav på samverkan och uppföljning av delegationerna. Samverkan i frågor om informationssäkerhet mellan enhetschefer, säkerhetschef, IT-chef, chefsjurist, representanter för systemägare och säkerhetssamordnare är lågfrekvent och knappast välutvecklad.

Ett tecken på brister i samverkan mellan dessa befattningstyper är att uppfattningen av begreppet informationssäkerhet skiljer sig mellan de intervjuade. Att enas om innebörden av begreppet är viktigt för en god samverkan och för en ändamålsenlig riskanalys.

Ett annat tecken på bristande samverkan ser Riksrevisionen i behandlingen av den utvärdering av SPV:s informationssäkerhetsarbete som

[30] SS-ISO/IEC 17799 är den väletablerade internationella standard som Riksrevisionen granskat mot.

beställdes av IT-enheten för cirka två år sedan.[31] Resultaten bör ha bedömts som oroande från beställarens sida samtidigt som den berörde frågor med betydelse långt utanför IT-enheten. Det hade då varit naturligt att få till stånd en bred analys och diskussion av åtgärder bland cheferna och andra roller inom myndigheten med arbetsuppgifter som avser informationssäkerhet. Detta skedde aldrig och flera av de som intervjuats under granskningen var knappast medvetna om rapportens existens och än mindre om dess innehåll.

8.2.2 Brister i riskanalysen

Begreppen riktighet/integritet och tillgänglighet samt i viss mån även spårbarhet förknippas inte på ett tydligt sätt med informationssäkerhet. Det medför att sekretessfrågorna tenderar att stå i fokus. Detta riskerar bl.a. att begränsa bredden på analysen av informationssäkerhetsriskerna vid SPV. Detta har sannolikt också medverkat till att flera intervjuade har uppfattningen att SPV:s information knappast är av intresse för omgivningen – undantaget vissa personer med skyddad identitet.

Tilliten till den egna personalen är stark bland cheferna. Att både interna och externa aktörer måste bedömas ha ett potentiellt intresse av att påverka parametrarna som styr beräkning av egna, närståendes eller stora gruppers pensionsbelopp är en uppfattning som inte delas av alla intervjuade. Att riktigheten hos de uppgifter som finns i SPV:s register därigenom skulle behöva betraktas som hotad både internt och externt har heller inte framgått på ett tydligt sätt i myndighetens riskanalyser. Riksrevisionen vill därmed inte påstå att SPV skulle sakna säkerhetsåtgärder som avser riktighet, tillgänglighet och spårbarhet. Det finns en mängd säkerhetsåtgärder som försvårar genomförande av hot på dessa områden. Fokus på sekretessfrågorna och bristerna i analyserna av interna och externa hot[32] ökar dock risken för att dessa typer av hot inte har behandlats tillräckligt ingående i riskanalyserna och att skyddet mot dem därmed kommer att eftersättas.

8.2.3 Brister i möjligheterna till överblick i informationssäkerhetsarbetet

Att skapa, upprätthålla och utveckla god informationssäkerhet är en svår uppgift i det alltmer komplexa hot- och riskpanorama som alla myndigheter möter. En väsentlig del av svårigheten ligger i behovet att överblicka och

[31] Riksrevisionen gör därmed ingen bedömning av kvaliteten i den utförda utvärderingen utan fokuserar på bristerna i kommunikation och styrning av informationssäkerhetsarbetet som hanteringen av utvärderingen och dess resultat visar på.

[32] Här avses främst uppsåtliga hot som riktas mot myndigheten av en angripare.

hantera en stor mängd företeelser, varav många förändras över tiden. SPV:s informationssäkerhetsarbete kräver överblick bl.a. över:

- vilka informationstillgångar som ska skyddas,
- vilka hot som ska prioriteras och avvärjas med skyddsåtgärder,
- vilka risker man får leva med och nöja sig med att lindra effekterna av,
- vilka skyddsåtgärder som redan införts och vilka svagheter (sårbarhet) som uppstått hos dem till följd av tillkommande hot,
- vilka tekniska förändringar i IT-miljö och rutiner som skett och som skapar ny sårbarhet,

För SPV:s del motsvaras dessa faktorer av tusentals företeelser som behöver överblickas i skilda delar av informationssäkerhetsarbetet. Det är därför med fog som LIS-standarden efterlyser stöd för att överblicka arbetsfältet. Det bör i en informationsbehandlande verksamhet av SPV:s omfattning och komplexitet finnas en databas som registrerar alla skyddsvärda informationstillgångar, vilka individuella krav på skydd som gäller för dem, vilka skyddsåtgärder som vidtagits för var och en av dem, vilka som ansvarar för tillgångarna, vilka beroendeförhållanden som finns tillgångarna emellan m.m.

På samma sätt behövs en övergripande plan över alla beslutade nya skyddsåtgärder (säkerhetsinvesteringarna), vilka som ansvarar för deras införande och korrekta funktion samt när de ska vara operativa. Inget av dessa behov av hjälpmedel för överblick finns väl tillgodosedda hos SPV. Behovet accentueras av de ovan beskrivna bristerna i information och samverkan i en komplex säkerhetsorganisation.

8.2.4 Brister i uppföljning och förvaltning av LIS

Riksrevisionen har vidare iakttagit brister i uppföljningen av delegationer som avser informationssäkerhetsfrågor. Hur väl genomförda säkerhetsåtgärder fungerar och hur väl SPV:s regelverk för informationssäkerhet efterlevs av anställda, konsulter och samarbetspartners klarläggs inte genom systematiskt uppföljning – dvs. med hjälp av ett uppföljningsprogram som beslutats av ledningen. Syftet med uppföljningen är bl.a. att ta fram ett underlag för förvaltningen av LIS. Förvaltningens syfte är i sin tur att stegvis förbättra LIS. De bristande möjligheterna till överblick tillsammans med bristerna i uppföljningen medför enligt Riksrevisionens mening att bedömningen av LIS ändamålsenlighet försvåras och att förvaltningen av LIS därför blir eftersatt. Tecknen på brister i förvaltningen av LIS utgörs bl.a. av att viktiga processer i informationssäkerhetsarbetet har brister utan att det finns tydligt beslutade åtgärder för att avhjälpa bristerna. De brister som åsyftas har redan berörts och avser möjligheterna till överblick i riskanalysen, utbildningsprocessen m.m.

8.2.5 Det saknas viktiga delar i SPV:s LIS

Till bristerna i möjligheterna till överblick, i riskanalysen och i utbildningsprocessen, kan läggas att en kontinuitetsplan för den lokala IT-miljön[33] saknas samt att väsentliga policier saknas – distansarbetspolicy – eller är mindre väl förankrade – informationssäkerhetspolicyn SPV:s LIS saknar därmed viktiga komponenter som stipuleras i LIS-standarden.

8.2.6 Sammanfattande bedömning

SPV har 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 – samverkan, riskanalys, utbildning samt uppföljning och förvaltning av LIS – eller saknas helt – lokal kontinuitetsplan, samlad åtgärdsplan, databas för överblick av informationstillgångarna samt distansarbetspolicy. Dessa brister medför att SPV:s LIS inte utgör en fullt ut lämpligt utformad och fungerande helhet. Vissa länkar i den kedja som ledningssystemets komponenter bilder saknas eller är för svaga. I praktiska termer innebär detta att bl.a. bristerna i samverkan i informationssäkerhetsarbetet, bristande överblick och brister i uppföljning och kontroll av LIS minskar SPV:s möjligheter att registrera de erfarenheter som gör ett systematiskt förvaltningsarbete möjligt. Med förvaltningsarbete avses här det styrda förbättringsarbete som syftar till att stegvis förbättra LIS.

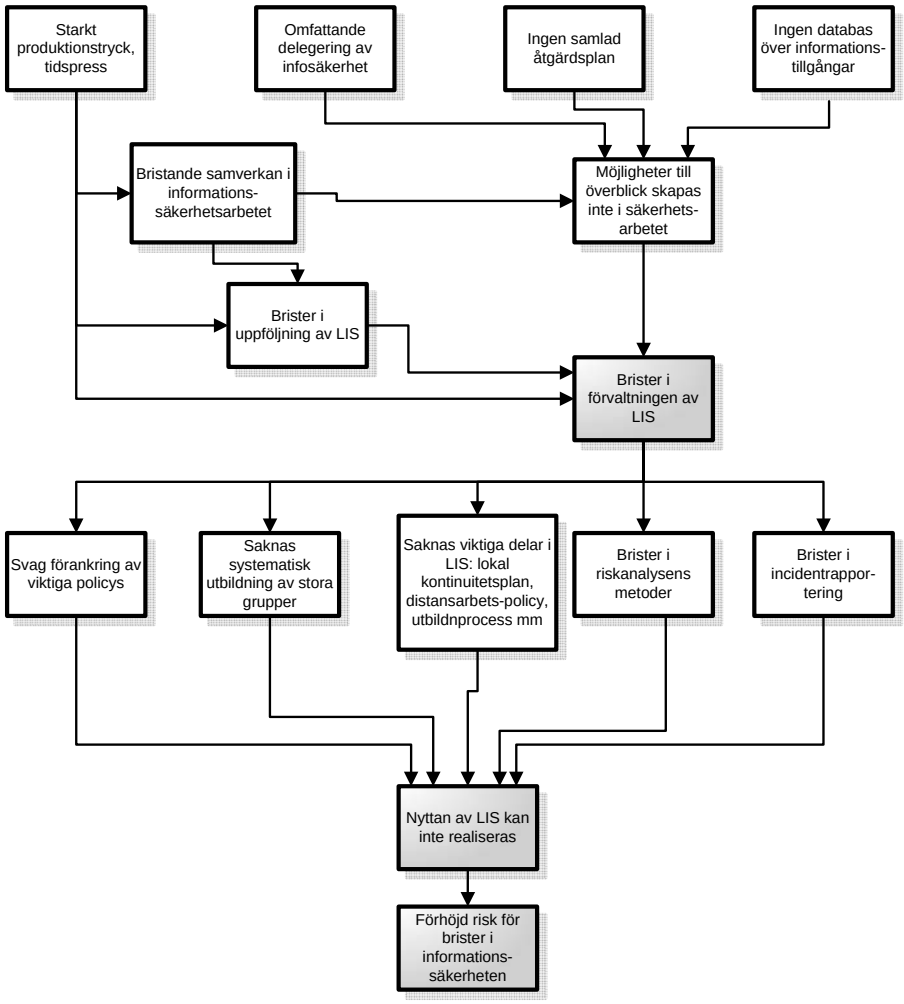
Bristerna i LIS påverkar i sin tur möjligheterna att uppnå och vidmakthålla eftersträvad informationssäkerhet.

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

En del av bristerna kan sannolikt kopplas till det starka produktionstrycket inom SPV – pensionsutbetalningarna måste genomföras under starkt uppbundna cykler. Det medför svårigheter att avsätta tid till annat, bl.a. uppföljning av kontrollers effektivitet och regelverkets efterlevnad samt förvaltning och vidareutveckling av myndighetens LIS.

[33] Den utkontrakterade stordatordriften har sin kontinuitetsplan.

Figur 2. Sambandsschema



En schematisk illustration av hur de ovan beskrivna bristerna i LIS påverkar SPV:s nytta av ledningssystemet framgår av figur 2. De faktorer som enligt Riksrevisionens bedömning medverkar till ”Brister i förvaltningen av LIS” återfinns i den övre delen av schemat. Av den nedre delen av schemat framgår att ”Brister i förvaltningen av LIS” medför att brister i SPV:s LIS inte upptäcks eller åtgärdas. Bristerna i LIS får som konsekvens att nyttan av LIS blir nedsatt, vilket i sin tur medför förhöjd risk för brister i den faktiska informationssäkerheten.

8.3 Rekommendationer

SPV:s ledning bör genomföra åtgärder för att komplettera sitt LIS i syfte att öka nyttan för myndigheten. 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 SPV stegvis ska kunna förbättra sitt LIS. Riksrevisionen rekommenderar därför att:

- SPV:s ledning kombinerar sin omfattande delegering av ansvaret för informationssäkerheten till systemägare med en systematisk uppföljning av att systemägarna tar sitt ansvar. Ledningens behov av stöd och metoder för denna uppföljning bör samtidigt ses över.
- SPV på ett mer systematiskt sätt bör följa upp bl.a. kontinuiteten i verksamhetens nyckelprocesser, personalens kompetens i informationssäkerhetsfrågor och efterlevnaden av regelverket för informationssäkerhet. Vidare bör den faktiskt uppnådda informationssäkerheten prövas. Behovet av stöd och metoder för denna uppföljning bör samtidigt ses över.
- SPV utvecklar riskanalysen med avseende på metodik, fokus och stöd. Med stöd avses en mer handfast hjälp med upplägg och genomförande av riskanalyser.
- SPV årligen sammanställer alla noteringar i systemförvaltningsplaner och andra dokument som avser beslutade säkerhetsåtgärder till en tydlig plan över beslutade åtgärder (åtgärdsplan) som används för genomförandet men också för återkommande uppföljning av vad som genomförts. Den bör tillsammans med ovan beskrivna riskanalys ge en samlad bild av risker, beslutade informationssäkerhetsåtgärder samt beräknade kostnader för dessa. Planens genomförande bör följas upp. Planen och dess uppföljning utgör ett viktigt underlag för ledningens styrning av arbetet med informationssäkerhet.
- SPV klargör arbetsuppgifter och ansvar för de skilda befattningstyper som är verksamma i informationssäkerhetsarbetet.
- Ledningsgruppen och övriga berörda går igenom och skapar gemensamma uppfattningar om vad begreppet informationssäkerhet och dess olika aspekter innebär för informationssäkerhetsarbetet.
- SPV prövar den faktiskt uppnådda informationssäkerheten när hotbilden, IT-miljön eller andra för informationssäkerheten väsentliga faktorer förändrats. Är förändringarna väsentliga eller svåra att bedöma bör insatser av extern expertis övervägas.
- SPV initierar en systematisk och återkommande utbildning och informationsförmedling inom området informationssäkerhet för olika personalkategorier.

Bilaga 1 SPV:s informationssystem och IT

Informationssystem/IT-stöd

- grunduppgifter/arbetsgivarregister
- Min arbetsplats/BizTalk/Web/Navet/Pensionsportal
- Förmåner, Premier, Skuld, SPÅ, P-skuld, Utbetalningsprognos, IÅP
- Kåpan/Kollekt/Mareg/ERF
- Utbetalning/Presys/Beviljanden
- Fam/Diabas

Statlig pensionsverksamhet

Projektet för utveckling av det nya systemstödet för administration av PA03 avslutades formellt. Den totala utvecklingskostnaden uppgår till ca 158 miljoner kronor. I september 2004 produktionssattes nya system för PA03. Fokus ligger nu på implementering av systemet.

Regeringen har bestämt att månatliga premier för PA03 ska införas fr.o.m. 1 januari 2005 i PA03.

Driftsättningen av PA03 innebär att SPV under flera år kommer att ha dubbla system för att klara hanteringen av samtliga pensionsavtal. Avskrivningstiden för PA03 är satt till tio år.

Pensionsportalen

Internetportalen www.minpension.se, som gör det möjligt för medborgarna att få en helhetsbild över sin framtida pension, sjösattes. Utvecklingen har skett i samarbete med Försäkringsförbundet, RFV, PPM och försäkringsbranschen. Portalen innebär också att e-signaturer används. SPV räknar med stort intresse för portalen och att antalet förfrågningar kommer att öka.

SPV:s hemsida

Den plattform som skapats rymmer både information, service och e-tjänster. Webbplatsen skapar förutsättningar för ökad öppenhet, tillgänglighet och

service till våra kunder, dessutom bidrar den till ett effektivt förvaltningsarbete. SPV har tagit steg mot framtidens e-tjänster genom utvecklingen av Rapport Direkt, vilket kommer att vara arbetsgivarens rapporteringsväg för anställningsuppgifter. En kartläggning av kunders förväntningar och behov har genomförts. Under 2005 kommer en anmälningsfunktion för utbildningar att bli tillgänglig, och kunderna kommer att kunna hämta fakturaspecifikationer.

Bilaga 2 Komponenter i SPV:s LIS[34]

Komponenter i LIS enligt webbenkäten	**SPV:s bedömning**
Aktuell sammanställning av informationstillgångar	Finns
Säkerhetsklassificering av den verksamhetskritiska informationen	Genomförd
Dokumenterad process för hantering av informationssäkerhetsrisker	Finns
Riskanalysrapport avseende säkerheten i den verksamhetskritiska informationen	Finns, 1–2 år gammal
Ledningssystem för informationssäkerhet	Finns, med vissa valda komponenter från SS 1 77 99
Detaljkomponenter i LIS (policy, känd fördelning av ansvar och befogenheter, incidentrapportering, plan för skyddsåtgärder, kontinuitetsplan, informationssäkerhetssamordnare, Internetpolicy, e-postpolicy, distansarbetspolicy, åtkomstpolicy, säkerhetskopiering, styrning av IT, hantering av PUL	Alla komponenter utom följande finns: distansarbetspolicy (ej aktuellt för SPV), hantering av PUL (planeras), utbildning för linjechefer och tidigare anställda (arbete pågår).
Utbildning/information, uppföljning av personalens kunskaper,	
Utvärdering, uppföljning och förvaltning av LIS.	

Kontrollmiljö

Ledningsgruppen	SPV:s ledning består av GD, ekonomichef, personalchef, chefsjurist, IT-chef, informationsdirektör, enhetschef Kund & Pension, enhetschef Försäkring samt pensionschef.
Ledningsgruppens agenda	Ledningsgruppens agenda omfattar olika IT-relaterade frågor, bl.a. frågor som rör informationssäkerheten. GD har varit aktiv i vissa IT-frågor och tagit initiativ till att problem utreds och åtgärdas.

[34] Uppgifter i dokument som SPV överlämnat till Riksrevisionen och intervjuer.

Möten i Ledningsgruppen med inslag av informationssäkerhet	Exempel på möten med IT-frågor: 2004-05-11 Information om projektstart för ny webbplats. Uppföljning av tidigare beslut i ledningsgruppen: reviderade styrdokument, systemanpassning, kontinuitetsplan för stordatordrift och lokal drift. Information om GD-beslut för 29 reviderade styrdokument. GD-beslut om översyn av information på G (?) – vilken information behöver lagras, struktur, skrivskydd, behörighet. GD-initiativ till att se över systemet för tilldelning av behörigheter till IT-systemen. Information om personalenkät om IT-stödet. Information om ev. nytt hem-pc-paket. Diskussion om beredskapen på IT-systemen under sommaren.
	2005-01-25 Gruppen informeras om bl.a. IT-katastrofplan, elektronisk fakturering. GD tar vissa beslut i anslutning till informationen
Säkerhetspolicy	En PM anger grunden för säkerhetsarbetet. Två områden behandlas – informationssäkerhet och fysisk säkerhet. PM förmedlar ett förhållningssätt, som ska genomsyra organisationen, till säkerheten.
Strategi och policy för säkerhetsarbetet	Broschyr från GD till alla anställda om vikten av att skydda informationen mot såväl avsiktiga som oavsiktliga hot.
Begrepp: Informationssäkerhet	Definitionen omfattar sekretess, riktighet, tillgänglighet och spårbarhet
Begrepp: Fysisk säkerhet	Skalskydd, inpasseringssystem, brand- och personlarm
Chefer i linjen	Ansvaret för säkerheten är en integrerad del i chefs- och linjeansvaret på olika nivåer. Detta gäller även för att genomföra och finansiera åtgärder som rör informationssäkerhet. Säkerhetschefen svarar för kostnaderna för fysiskt skydd.
GD	GD har det övergripande ansvar för säkerheten. GD har delegerat vissa beslut.
Säkerhetsorganisation	Organisationen omfattar säkerhetschef, tillika operativt ansvarig för den fysiska säkerheten, IT-chef samt säkerhetssamordnare,
Säkerhetsråd	Säkerhetschef (sammankallande) och säkerhetssamordnare. Forum för informationsutbyte.
Verksamhetsansvarig	Verksamhetsansvarig svarar för att hela verksamhetens IT-stöd har rätt säkerhetsnivå. Uppmärksammar och anmäler personalens behov av behörigheter till IT-system. Ansvarar för att de personer som får tillgång till IT-system m.m. i IT-miljön uppfyller de förutsättningar som gäller för behörighet. Uppmärksammar säkerhetsfrågor och för dem vidare till säkerhetschefen.
Systemägare	Ägare av enskilda IT-system. Ansvarar för att ställa krav på, införa skydd och upprätthålla skyddet för systemet.
Systemförvaltare	Rollen som systemförvaltare finns på leverantörssidan. I rollen ingår ändringshantering (akut), förbättring och produktion samt testning av system.
Systemleverantörsrepresentant	Huvudansvarig för att systemet håller den nivå på informationssäkerhet som beslutats av verksamheten. Genomför regelbundna risk- och sårbarhetsanalyser.
Driftbeställare, teknikbeställare	Huvudansvarig för att lämna information angående driftstörningar i systemet och/eller IT-stödet och rapportera dessa till systemförvaltaren.
Konstruktörsansvarig, konstruktör + andra	Huvudansvarig för testmiljö, tester, godkänna acceptanstester.
Särskild säkerhetsorganisation med säkerhetschef och säkerhetssamordnare (8 st)	Säkerhetsorganisationen arbetar med fysisk säkerhet och informationssäkerhet. Säkerhetschefen har tillsyns- och samordningsansvar. Han tar fram underlag bl.a. riskanalyser, vakar/granskar över åtgärder, informerar, samlar information om läget, bevakar incidentrapporteringen m.m. Rapporterar direkt till GD. Tar fram årlig budget för beslutade säkerhetsåtgärder.

IT-chef	IT-chef ansvarar för behörighetssystem, kontinuitetsplan och test av denna, datorkraftleverantör uppfyller säkerhetskraven.
Samarbete mellan säkerhetschefen, verksamhetsansvariga, systemägare och IT-chef	Arbete med informationssäkerhet.
Samarbete mellan säkerhetschef och den operativt ansvarige på Internservice	Arbete med fysisk säkerhet.
Användare av system	Användare ska ha (godkänd) kunskap om säkerhetsregler. Svarar själv för att följa de regler som kopplas till aktuell behörighet. Ska rapportera incidenter och tillbud.

Riskhantering

Programförteckning	En lista finns över programvaror
Viktiga informationssystem och strategiskt IT-stöd	Två PM finns om säkerhetsprioritering. Av säkerhetsprioriteringen framgår vilka system som är mest prioriterade.
Skyddsvärda områden	IT-system, medarbetare, konsulter, underleverantörer, anläggningar, byggnader.
Informationsklassificering	En föreskrift finns. SPV ska alltid klassificera sin information. Informationens känslighet för att skador kan uppstå om information kommer i orätta händer eller IT-stöd slås ut. Frågor om sekretess och tillgänglighet är i fokus. Klassificeringen är en grund för val av skyddsnivå. Anger vem som ansvarar, när och hur. Systemägaren är ansvarig.
Scenario över tillbud	Två dokument finns med inriktning på säkerhetsprioritering för verksamhetssystem (Kund & Pension, Försäkring). Scenarier: 1) systemen går ned och måste tas upp i en viss ordning, 2) verksamhet måste kunna bedrivas utan att systemen fungerar.
Risk- och sårbarhetsanalys	Varje chefs säkerhetsansvar omfattar bl.a. att verka för att kontinuerliga riskanalyser utförs. Viktiga riskkällor ska uppdateras årligen som underlag för val av skyddsåtgärder för att minska sårbarheten. SPV anser att det är onödigt att göra årliga riskanalyser. PM 2005-02-01 Fokus på kris- och katastrofplan, IT-katastrofplan, säker drift i lokal miljö, bättre behörighetssystem (vid e-tjänsterna, e-legitimation), säker telekommunikation (kryptering), vägledning för val av skyddsnivå. PM 2003-12-16 Fokus på tänkbara händelser/hot/risker (dataintrång, telekommunikation, virus, sabotage, nyckelpersoner, bedrägerier, etc. Starka uttalanden om att säkerställa kontinuiteten i verksamheten. Lista över de största hoten (virus och dataintrång är 4 och 5). Citat: ”Det finns idag ingen övergripande kontinuitetsplan inom SPV. Vissa delar, såsom det centrala IT-stödet, är säkrat men ser man till helheten finns det stora förbättringsmöjligheter”. PM 2003-10-30 Fokus på IT-miljön på SPV baserat på ISO 17799 (LIS). Workshopform. OK till fysiskt skydd, vissa skyddsåtgärder i IT-miljön. *Ett 30-tal viktiga brister identifierades utifrån LIS*. Det gäller att säkerhetsregler inte är förankrade i organisationen, kontinuitetsplaner saknas, säkerheten byggs inte in i IT-projekten från början. Ett åtgärdsprogram har tagits fram per brist. Vidare anges hur SPV ska arbeta med säkerhetsfrågorna framöver.

Analysdokument – riskanalys; metod för riskanalys	Subjektiv metod för att göra analys som är snabb och visuell (vitala resurser och klassificering, hot (organisatoriska, fysiska, logiska), hotens sannolikhet och konsekvens, prioritering av hot/risker, val av skyddsåtgärder).
Skyddsnivå	Skyddsnivån finns preciserad för viktiga system och IT-stöd.
Åtgärdsplan	Underlag för sådan finns i PM Risk- och sårbarhetsanalys. Främst i 2003-10-30. Genomförda åtgärder: övergripande Kris- och katastrofplan (särskild organisation), IT-katastrofplan.

Kontrollfunktioner

Informationssäkerhetspolicy	Policyns syfte att säkerställa SPV:s verksamhet mot avbrott gäller all informationshantering. Fokus är på informationens tillgänglighet, riktighet, sekretess och spårbarhet. Skyddsåtgärder för dessa ska finnas. Säkerhetsansvaret ligger i verksamhetsansvaret.
Verksamhetskrav – behörigheter	Krav ställs på behörigheter i nya system. Krav ställs på IT-stöd för behörighetsadministration (interna eller externa användare, olika roller, grupper samt sekretess).
Föreskrift för tilldelning av behörighet	Reglering av tilldelning av behörighet till informationssystem inkl. bilder från RFV och lokala nätverk. Föreskrifterna omfattar SPV:s personal, tillfälligt anställda, konsulter samt externa kunder. Föreskrifterna är en del av SPV:s skyddsåtgärder avseende sekretess och tillgänglighet i enlighet med SPV:s informationssäkerhetspolicy.
Sekretess	En PM finns med precisering av försiktighet i hantering av känslig information. En PM finns om hantering av sekretessmarkerade individer i pensionshandläggningen. En PM finns om loggning av åtkomst till sekretessbelagd information.
Behörighet – kontroll	Datasystemen är utrustade med behörighetskontrollsystem. För att bli behörig krävs godkännande av chef och ev. från systemägare. Behörighetskontrollen omfattar lösenord. För vissa system gäller även andra regler.
Loggar	Systemen har loggfunktioner för att kunna spåra ev. intrång från obehöriga.
Kontroll av loggar	Verksamhetsansvarig ska, om en transaktion är extra känslig ur säkerhetsskyddssynpunkt, vidta extra skyddsåtgärder, t.ex. regelbunden uppföljning av loggar.
Lagring	Lagring av verksamhetskritisk information ska ske på gemensamma diskutrymmen, bl.a. för att underlätta säkerhetskopiering. Är information lokalt lagrad, svarar den enskilde för säkerhetskopieringen.
IT-katastrofplan	Det finns en katastroforganisation som träder i kraft när katastrof inträffar. Organisationen har i förväg planerade åtgärder. En uppgift är att få fram hot.
Rutiner för rapportering vid incidenter	Begreppet incident är definierat. En PM finns med exempel på incidenter. Vem som rapporterar till vem och hur. Rutin och incidentrapport finns på Navet resp. mall i WORD. Av föreskrifter för tilldelning av behörighet framgår att alla inom SPV är skyldiga att meddela berörd chef vid misstanke eller upptäckt av att behörighetssystemet inte fungerar tillfredsställande, obehörig användning av användar-id, vid ev. virusangrepp, etc. Om bristen kan innebära eller har inneburit skada för SPV ska detta anmälas till säkerhetschefen eller GD.

Internetpolicy	Ansvaret för efterlevnaden är direkt kopplat till varje medarbetare. Internetpolicyn finns i intranätet Navet.
Policy för e-post	e-postpolicyn finns i intranätet Navet. Arbetsgivaren är ansvarig för att utbilda alla i policyn. Ansvaret för efterlevnaden är direkt kopplat till varje medarbetare.
Bärbar dator	Särskilda säkerhetsregler. Det är den enskilde användarens ansvar att skydda dator och information i den enligt de regler som finns.
Utrustning	Enbart SPV:s utrustning får kopplas in på nätet.
Kopiering/nedladdning av programvaror	Privat kopiering är olagligt och får inte förekomma inom SPV. Rätten till kopiering regleras av programvaruleverantören. Original och säkerhetskopia ska förvaras i datamediaskåp. Det är inte tillåtet att ladda ned program, spelprogram och filer från Internet.
Kassering/utplåning	IT-enheten ska alltid tillfrågas innan en dator kasseras eller sänds på reparation. Känslig information tas bort från hårddisken.
Fysiskt skydd	Brandlarm, inbrottslarm, kontroll vid in- och utpassering.
Systemutveckling	Säkerheten ska finnas med från början.
Projektkontrakt	Skapa styrning och kontroll av projekt i form av ett kontrakt mellan projektbeställaren och projektledaren.

Information och utbildning

Utbildning	Särskild utbildning ges i säkerhet 2–3 gånger per år. Utbildningen omfattar säkerhetspolicy, säkerhetsföreskrifter, säkerhetsrutiner, lagar, etik och moral.
Information	En särskild informationsskrift ”Säkerhet på SPV” ges till alla som anställs vid SPV. Säkerhetschefen har ett särskilt presentationsmaterial som används då säkerhetschefen informerar.
Krav på kompetens	Behörighet till IS-system får endast den som har tillräcklig kompetens för att arbeta med systemet. Verksamhetsansvarig är ansvarig för att personalen uppfyller kompetenskraven. Det är chefens skyldighet att se till att personalen får nödvändig utbildning för att få möjlighet att följa de regler och instruktioner som finns vid SPV.

Uppföljning, utvärdering och förvaltning av LIS

Uppföljning	SPV:s uppföljning och utvärdering av sin LIS sker främst i arbetet med risk- och sårbarhetsanalys, och därvid i särskild ordning i PM 2003-10-30.
	Vidare följer GD och ledningsgruppen upp arbetet med vissa åtgärder från nämnda PM.

Källförteckning

Lagstiftning

Tryckfrihetsförordning (1949:105)

Arkivlagen (1990:782)

Personuppgiftslagen (1998:204)

Sekretesslagen (1980:100)

Skyddslagen (1990:217)

Lag (2003:389) om elektronisk kommunikation

Förordningar

Arkivförordningen (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)

Verksförordningen (1995:1322).

Rikspolisstyrelsens föreskrifter om säkerhetsskydd (RPS FS 1996:9 FAP 244-1)

Texter från Internet

Mörkertalsundersökningen. Hämtat 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 Canada. 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)