RIKSREVISIONEN

Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten

ISBN 91 7086 092 0
RiR 2006:24
Tryck: Riksdagstryckeriet, Stockholm 2006

Till regeringen
Näringsdepartementet

Datum 2006-11-29
Dnr 31-2006-0310

Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten

Riksrevisionen har granskat den interna styrningen och kontrollen av informationssäkerheten vid Arbetsmarknadsverket. Granskningen ingår i en serie av granskningar som genomförs vid statliga myndigheter avseende informationssäkerhet. Resultatet av granskningen redovisas i denna rapport.

Företrädare för Arbetsmarknadsstyrelsen har beretts tillfälle att fakta-granska och lämna synpunkter på utkast till denna granskningsrapport.

I enlighet med 9 § lagen (2002:1022) om revision av statlig verksamhet överlämnas rapporten till regeringen. Rapporten överlämnas samtidigt till Riksrevisionens styrelse.

Granskningsrapporten innehåller slutsatser och rekommendationer som avser Arbetsmarknadsverket och överlämnas därför även till Arbetsmarknadsstyrelsen.

Riksrevisor *Karin Lindell* har beslutat i detta ärende. Granskningen har genomförts av revisionsledare *Karin Upplander Ekman* (föredragande), revisionsdirektör *Bengt E W Andersson* och revisor *Ulrika Meyer*. Biträdande granskningsområdeschef *Rutger Banefelt* och revisionsdirektör *Björn Undall* har medverkat i den slutliga handläggningen.

Karin Lindell

Karin Upplander Ekman

För kännedom:
Arbetsmarknadsstyrelsen

Innehåll

Sammanfattning

Nästan en tredjedel av alla offentliga organisationer har utsatts för någon form av allvarligt dataintrång eller virusangrepp. Angreppen blir alltmer avancerade och allvarligare. 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 IT-stödet för verksamheten. Det är ett arbete som är både svårt och ofta resurskrävande. Det är mot denna bakgrund som Riksrevisionen har ökat sina insatser för att granska informationssäkerheten inom staten.

Ansvaret för styrning och ledning av statsförvaltningens informationssäkerhet är fördelat mellan riksdagen, regeringen, de av regeringen utsedda tillsyns- och stödmyndigheterna samt de enskilda myndigheternas ledningar. Riksrevisionen har i denna granskning valt att fokusera på hur myndighetsledningen tar sitt ansvar för informationssäkerheten.

Under åren 2005–2006 har Riksrevisionen granskat informationssäkerheten vid tio statliga myndigheter. Denna granskning fokuserar på hur Arbetsmarknadsverket (AMV) har arbetat 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 gå att fastställa vem som använt informationen och ändrat den.

Riksrevisionen har i sin granskning utgått från en internationell standard, den s.k. LIS-standarden (SS-ISO/IEC 17799). LIS-standarden beskriver hur ett väl fungerande ledningssystem för informationssäkerhet bör vara utformat.

Denna standard täcker alla de områden som säkerhetsarbetet bör 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?

AMV:s IT-system måste kunna hantera mycket stora penningströmmar och stora volymer integritetskänsliga uppgifter om ett mycket stort antal enskilda personer samt uppgifter om företag och lediga platser.

Vid arbetsförmedlingen fanns under år 2005 närmare 720 000 olika personer som vid något tillfälle registrerats som arbetslösa. Det anmäldes 430 000 lediga platser och ungefär 415 000 placeringar i arbetsmarknadspolitiska program genomfördes vid förmedlingarna. Antalet övergångar till arbete har legat på 630 000 per år de senaste fem åren. Utgifterna för AMV under budgetåret 2005 uppgick till ca 67 miljarder kronor.

Arbetsförmedlingens Internettjänster har successivt byggts ut. Antalet unika besökare på arbetsförmedlingens webbplats har ökat från ca 700 000 år 2002 till drygt 1,5 miljoner bara under det första kvartalet år 2006.

Det ställs stora krav på att den information som finns i AMV:s informationssystem är skyddad: att informationens riktighet, tillgänglighet, sekretess och spårbarhet är skyddade. Felaktiga uppgifter i AMV:s register till följd av bristande informationssäkerhet kan få omfattande konsekvenser.

Några exempel på tänkbara konsekvenser av brister i informationssäkerheten är:

- att sekretessbelagda personuppgifter röjs,
- att enskild person lider ekonomisk skada då underlag till a-kassa är fel och beslut fattas på felaktiga grunder,
- att statistikunderlag och uppföljningar till bl.a. regering och riksdag blir missvisande,
- att matchning av arbetssökande med arbetsgivarnas lediga platser inte får full effekt på grund av bristfällig registerkvalitet.

Har Arbetsmarknadsverket ett väl fungerande ledningssystem för informationssäkerhet?

Granskningen visar att ledningens informationssäkerhetsarbete vid AMV har tre väsentliga brister som påverkar ledningens förmåga att genomföra beslutade säkerhetsnivåer och verka för att de bibehålls inom myndigheten. Dessa brister rör ledningens styrning och kontroll av informationssäkerhetsarbetet, arbetet med en samlad riskanalys samt ledningens uppföljning och vidareutveckling av ledningssystemet för informationssäkerhet. Mer konkret kan följande brister omnämnas. Flera ledningsbeslut som rör de verksamhetsansvarigas arbete med

informationssäkerheten har inte genomförts. Det finns ingen samlad åtgärdsplan för säkerhetsarbetet. Någon utbildning i informationssäkerhet har inte genomförts. Behovet av att förbättra ledningens arbete med informationssäkerheten har inte initierats från ledningen utan från personal i organisationen och från utomstående.

Bristerna avser väsentliga punkter i ledningssystemet. Sammantaget bedömer Riksrevisionen att AMV utifrån gängse normer inte fullt ut arbetar systematiskt med sitt ledningssystem för informationssäkerhet. Konsekvenserna av bristande informationssäkerhet kan bli allvarliga, som framgår ovan.

Riksrevisionens rekommendationer

Riksrevisionens bedömning är att ett sammanhållet och tydligt ledningssystem för informationssäkerhet är en förutsättning för att AMV:s ledning ska kunna förvissa sig om att beslutade säkerhetsnivåer införs och bibehålls i hela myndigheten. Detta kräver bl.a. att ledningssystemet omfattar hela AMV och är integrerat med övriga ledningssystem. Det bör ge ledningen möjlighet till överblick över risker och skillnader i risker mellan olika verksamheter, behovet av säkerhetsåtgärder och kostnader för säkerhetsarbetet i de olika verksamheterna. Då framstår också tydligare vilket utrymme som finns för prioriteringar mellan säkerhetsinvesteringar i skilda delar av myndigheten. Den i granskningen använda LIS-standarden innehåller enligt Riksrevisionens bedömning de viktigaste kraven på ett sådant ledningssystem.

En viktig utgångspunkt är att AMV måste kunna garantera medborgare och företag att uppgifter i IT-systemen hanteras säkert. AMV:s ledning bör vidare ställa krav på sitt ledningssystem som beaktar de allvarliga konsekvenser som kan inträffa om IT-systemen inte är säkra. AMV har nyligen påbörjat ett viktigt arbete med att förbättra sitt ledningssystem för informationssäkerhet.

Riksrevisionen rekommenderar AMV att beakta nedanstående i arbetet med att förbättra ledningssystemet.

- Ledningen bör utforma sitt ledningssystem för informationssäkerhet så att den kan förvissa sig om att beslutade säkerhetsnivåer införs och bibehålls i hela myndigheten. I detta bör ingå att precisera och fastställa hur säkerhetsarbetet ska bedrivas och därvid tydliggöra ansvarsfördelning, samordning, utbildningsinsatser och rapporteringsvägar inom organisationen.

- I AMV:s ledningssystem bör ingå en systematisk process för myndighetens riskanalysarbete. En sådan process skulle ge ledningen möjlighet att överblicka risker för hela AMV, skillnader i risker mellan olika verksamheter, behov av säkerhetsåtgärder och kostnader för säkerhetsarbetet i de olika verksamheterna. Då framträder tydligare vilket utrymme som finns för prioriteringarna mellan säkerhetsinvesteringar i skilda delar av myndigheten. Dessa prioriteringar bör samlas i en åtgärdsplan. Ledningen bör med denna plan följa upp att beslutade åtgärder införs och fungerar som avsett. Den bör vidare utformas så att de resurser som ägnas säkerhetsarbetet kan beskrivas, följas och utvärderas.
- Ledningen bör systematiskt följa upp hur ledningssystemet fungerar, och om de förutsättningar och krav som ledningssystemet bygger på är uppfyllda och aktuella. Detta bör ske som en del av en strategi för vidareutveckling av ledningssystemet.

1 Inledning

1.1 Bakgrund, syfte och revisionsfrågor

1.1.1 Bakgrund

Under åren 2005–2006 har Riksrevisionen granskat informationssäkerheten på tio statliga myndigheter[1]. Denna granskning avser Arbetsmarknadsverkets (AMV) informationssäkerhet.

Informationssäkerhet[2] omfattar

- konfidentialitet/sekretess, vilket betyder att endast behöriga användare kommer åt informationen i verksamhetens informationssystem,
- tillgänglighet, vilket betyder 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), vilket betyder att information inte obehörigt ändras eller modifieras,
- spårbarhet, vilket betyder att kunna se vem som gjort vad och vid vilken tidpunkt, exempelvis om informationen påverkats i strid med myndighetens regler.

Informationssäkerheten är allt svårare att upprätthålla hos myndigheterna i takt med att deras verksamhetsprocesser utvecklas mot alltmer sammanvävda IT-system med kopplingar till andra myndigheter och till enskilda och företag via Internet. Elektronisk förvaltning, dvs. elektroniska tjänster till enskilda och företag, får insteg hos de flesta statliga myndigheter och därigenom vidgas tjänsternas användningsområde och användbarhet. Allt större krav ställs på att dessa tjänster är säkra, inte minst för att medborgare och företag ska ha förtroende för dem, Med denna utveckling följer bl.a. att myndigheterna löpande behöver se över och vid behov förstärker skyddet mot de risker som uppstår.

---

[1] Sex granskningar har gjorts utifrån den presenterade metoden och publicerats som granskningsrapporter: Sjöfartsverket, Statens Pensionsverk, Försäkringskassan, Lantmäteriverket, Migrationsverket och Arbetsmarknadsverket. Metoden har i vissa delar tillämpats i ytterligare fyra granskningar, som har rapporterats på annat sätt: Bolagsverket, Försvarsmakten, Post- och telestyrelsen samt Svenska Kraftnät

[2] Enligt ISO 17799.

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

- 21 procent av statliga och kommunala myndigheter 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 procent av statliga och kommunala myndigheter har varit med om IT-säkerhetsincidenter som inneburit att en angripare gjort en utförlig kartläggning av organisationens system, dvs. att obehörig letat efter sårbara punkter.
- 20 procent av statliga och kommunala myndigheter har varit med om IT-säkerhetsincidenter som medfört att system eller delar av system blev otillgängliga, s.k. DOS-angrepp eller Denial of Service. Ett exempel är när system eller nätverk blivit överbelastade på grund av ett DOS-angrepp.
- 30 procent av statliga och kommunala myndigheter har varit med om IT-säkerhetsincidenter som inneburit ett allvarligt utbrott av skadlig kod med betydande konsekvenser för verksamheten. Som exempel kan nämnas s.k. virus, maskar, och trojaner.

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

1.1.2 Syfte

Ansvaret för styrning och ledning av statsförvaltningens informationssäkerhet är fördelat mellan riksdagen, regeringen, de av regeringen utsedda tillsyns- och stödmyndigheterna samt de enskilda myndigheternas ledningar. Riksrevisionen har i denna granskning valt att fokusera på hur myndighetsledningen tar sitt ansvar för informationssäkerheten.

Riksrevisionen har vidare valt att avgränsa granskningen till arbetet med säkerheten för de IT-relaterade informationstillgångarna. Därmed granskas inte säkerheten för manuella register, brev och liknande informationssamlingar[4]. Skälet till detta 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.

---

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

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 därför 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. Denna avgränsning innebär bl.a. att faktiskt uppnådd säkerhet i enskilda system inte granskats. Däremot har Riksrevisionen tagit del av rapporter som avser skyddet i vissa enskilda system. God informationssäkerhet kräver ett systematiskt säkerhetsarbete som leds utifrån noggranna analyser av bl.a. verksamhetens säkerhetsbehov, sårbarhet och risker. Ett väl fungerande ledningssystem för informationssäkerhet är alltså en viktig förutsättning för god informationssäkerhet.

Betydelsen av ledningssystemet som förutsättning för god informationssäkerhet är särskilt stor i omfattande och komplexa verksamheter med stora och svåröverblickbara IT-system. Detta är bakgrunden till Riksrevisionens val av ledningssystem för informationssäkerhet som fokus för denna granskning.

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

1.2 Bedömningskriterier

I bedömningen av AMV:s styrning och ledning av informationssäkerhetsarbetet har Riksrevisionen utgått från ett flertal normer och standarder[5]. Standarden Ledningssystem för informationssäkerhet – Riktlinjer för ledning av informationssäkerhet (SS-ISO/IEC 17799 och SS 627799) är grunden för Riksrevisionens granskningskriterier. Denna standard (i fortsättningen kallad LIS-standarden[6]) innehåller riktlinjer som enligt standarden ”bör betraktas som ett underlag för att utveckla organisationsspecifika riktlinjer. Allt som

[5] Standarden Ledningssystem för informationssäkerhet, Krisberedskapsmyndighetens rekommendation BITS, Basnivå för IT-säkerhet, verksförordningen (1995:1322), förordning om myndigheters riskhantering (1995:1300), förordning om krisberedskap och höjd beredskap (2006:942), 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.

[6] I rapporten används begreppet LIS-standarden när de normkällor avses som Riksrevisionen utgått från, vilka nämns ovan (SS-ISO/IEC 17799 och SS 627799). Vidare används i rapporten begreppet ledningssystem när Riksrevisionen beskriver myndighetens eget ledningssystem för informationssäkerhet.

nämns i LIS-standarden är kanske inte tillämpligt. Ytterligare åtgärder, som inte anges i denna standard, kan också vara nödvändiga."[7]. Samtidigt utgör standarden "en gemensam grund för i princip alla organisationer."[8]

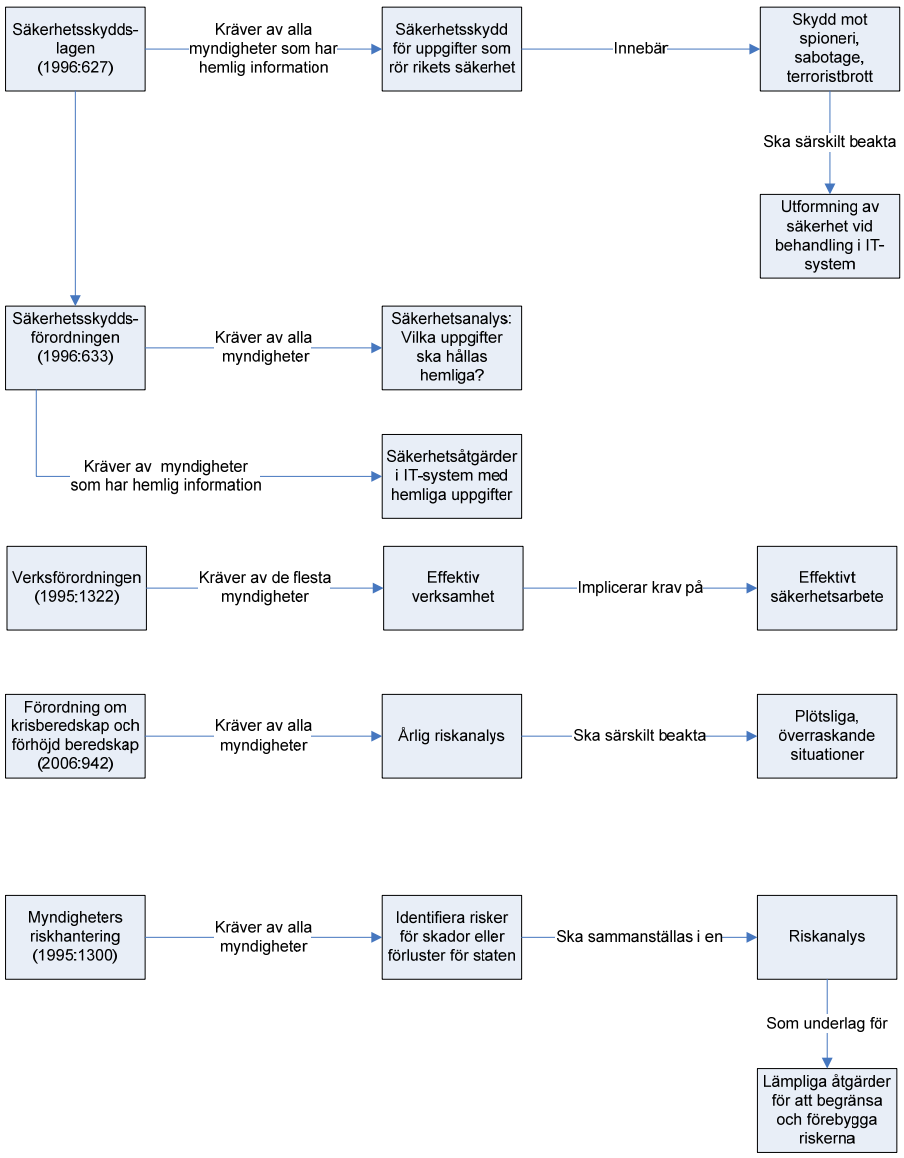
För Riksrevisionens beslut har följande faktorer haft betydelse:

- LIS-standarden är den mest heltäckande standarden för informationssäkerhet. Den täcker alla länkar 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 riktlinjer har visats sig vara stabila. Standarden har efter tio år nu uppdaterats beträffande sin disposition men den är innehållsmässigt intakt.

1.2.1 Översikt av lagar och förordningar som berör informations-säkerhet

Lagar och förordningar som berör informationssäkerhetsområdet beskrivs i figuren nedan. De behandlar myndigheters riskhantering (förordning [1995:1300] om myndigheters riskhantering), åtgärder för fredstida krishantering (förordning [2006:942] om krisberedskap och höjd beredskap) samt skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet (säkerhetsskyddslagen [1996:627]).

[7] SS-ISO/IEC 17799 s 10.
[8] SS-ISO/IEC 17799 s 10.



Figur 1. Översikt över reglering av informationssäkerhet.

Vad som berör **samtliga myndigheter** i dessa författningar är

- kravet att årligen analysera om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Särskilt ska beaktas situationer som uppstår hastigt, oväntat och utan förvarning eller situationer där det finns ett hot, eller en risk att ett sådant läge kan komma att uppstå samt situationer som kräver brådskande beslut och samverkan med andra aktörer. Myndigheterna ska vidare särskilt beakta att de mest nödvändiga funktionerna kan upprätthållas i samhällsviktig verksamhet, och att förmågan att hantera mycket allvarliga situationer inom myndighetens ansvarsområde upprätthålls (9 § förordning om krisberedskap och höjd beredskap).

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 mot exempelvis spioneri och terroristbrott 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 arbete med informationssäkerhet 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 för den hemliga informationen. Förordning om myndigheters riskhantering innehåller därmed implicit ett krav på riskanalys också beträffande informationssäkerhet. Vidare krävs att lämpliga säkerhetsåtgärder vidtas för att begränsa och förebygga riskerna. Riksrevisionen uppfattar därför förordningen om myndigheters riskhantering som den mest heltäckande författningen när det gäller krav 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.

Enligt Riksrevisionens tolkning av LIS-standarden ska, enligt den enskilda myndighetens bedömning, all *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 LIS-standarden ligger i linje med 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, men täcker även områden som inte direkt reglerats i lagar och förordningar.

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. Eftersom LIS-standarden innehåller de mest väsentliga kraven på ett sådant ledningssystem har Riksrevisionen tagit fram ett granskningsprogram med kriterier och intervjufrågor som avser myndighetens ledningssystem och som baseras på standarden. Frågorna har strukturerats efter den interna styrningen och kontrollens olika beståndsdelar enligt den s.k. COSO-modellen[9]. Granskningsprogrammet har behandlats i seminarier med Swedish Standards Institute, Krisberedskapsmyndigheten (KBM), Statskontoret och en säkerhetschef inom bank- och försäkringssektorn.

Standarden är omfattande och Riksrevisionens frågor till myndigheten har därför baserats på ett urval i syfte att fånga de mest väsentliga kraven på ledningssystemet. Urvalet kommer också till uttryck i de bedömningskriterier som inleder kapitlen 3-7. Urvalet har behandlats vid de ovan nämnda seminarierna.

Det bör framhållas att det inte finns några formella krav på att en myndighet ska uppnå en viss nivå enligt LIS-standarden. Ytterst är det myndighetens ledning som avgör ambitionsnivån.

[9] 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. Kapitlen 3 - 7 i Riksrevisionens rapport anknyter till dessa beståndsdelar.

1.3 Metoder och tillvägagångssätt i granskningen

Granskningen påbörjades i april 2006 och har genomförts på följande sätt:

- AMV valdes ut för granskning på grund av sin mycket omfattande hantering av information om enskilda och företag, samt för sin betydelse i samhällsekonomin. Riksrevisionen hade alltså ingen information om eventuella brister i myndighetens informationssäkerhet som påverkade valet.
- Myndigheten har först fått ett introduktionsbrev och en begäran att förse Riksrevisionen med styrdokument inom området, bl.a. informationssäkerhetspolicy. Introduktionsbrevet sändes till AMV den 30 mars 2006. Ett introduktionsmöte om granskningen hölls på Arbetsmarknadsstyrelsen (AMS) den 7 april 2006 varefter en första översiktlig intervju genomfördes med IT-säkerhetssamordnare, inklusive en diskussion om förekomst av dokument.
- Myndigheten har därefter fått besvara en enkät i form av en självutvärdering om myndighetens syn på sin verksamhet och behovet av informationssäkerhet. Myndigheten har i enkäten vidare redovisat 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 över nyckeldokument som Riksrevisionen behövt för sin granskning. Myndigheten har sedan översänt dessa (se bilaga 3). Myndigheten har gjort en egen bedömning vilka av dessa 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 AMS respektive länsarbetsnämnderna blivit intervjuade[10] med stöd av granskningsprogrammets intervjufrågor. Eftersom AMV har en stor regional och lokal organisation, har intervjuer även genomförts vid två länsarbetsnämnder. Intervjuerna har genomförts i maj och juni 2006. Under intervjuerna har den problembild som successivt vuxit fram tagits upp med och kommenterats av den intervjuade. Efter intervjuerna har en del kompletterande dokument överlämnats till revisionen.
- Myndigheten har sedan (under oktober 2006) faktagranskat utkastet till revisionsrapport.

[10] Generaldirektör, ställföreträdande generaldirektör, cheferna för avdelning för arbetsförmedlingsfrågor, internrevision och IT-enheten, IT-säkerhetssamordnare, handläggare på AMS och IT-metodare på länsarbetsnämnder.

1.4 Läsanvisningar

Begreppet ”systematisk” används på flera ställen i den följande texten. Det står för ett förfarande som till sin natur är metodstyrt och överlagt.

Ett annat ord som används är ”tillräcklig”. Det är en bedömning som Riksrevisionen gör av hur långt AMV kommit i förhållande till Riksrevisionens tolkning[11] av de krav som uttrycks i LIS-standarden.

I rapporten har redovisningen av granskningskriterier, iakttagelser och slutsatser strukturerats i enlighet med COSO-modellen:

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

En beskrivning av Riksrevisionens bedömningskriterier för respektive komponent i COSO-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 på 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 att det kan vara av värde för AMV i exempelvis 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.

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

2 Arbetsmarknadsverket och informationssäkerheten

2.1 Arbetsmarknadsverkets verksamhet

I Sverige finns en offentlig arbetsförmedling. Denna förmedling finns hos AMS och länsarbetsnämnderna. AMV består av AMS, som är chefsmyndighet, och en länsarbetsnämnd i varje län samt ca 320 lokala arbetsförmedlingar. Totalt arbetar drygt 10 000 personer inom AMV.[12]

Stödet från arbetsförmedlingen lämnas genom tre kanaler: Arbetsförmedlingen Internet (ams.se), Arbetsförmedlingen kundtjänst (telefonservice) samt den lokala arbetsförmedlingen. En huvuduppgift är att sammanföra den som söker arbete med den som erbjuder arbete. Totalt erbjuder förmedlingen nio olika typer av tjänster, riktade till enskilda personer och arbetsgivare. Arbetsförmedlingen bedriver även vägledning, arbetslivsinriktad rehabilitering och förmedling av arbetsmarknadspolitiska program. Den kontrollerar också att de arbetslösa står till arbetsmarknadens förfogande och därigenom har rätt till arbetslöshetsersättning.

Under år 2005 fanns närmare 720 000 olika personer registrerade vid något tillfälle som arbetslösa[13]. Det anmäldes 430 000 lediga platser och ungefär 415 000 programplaceringar genomfördes vid förmedlingarna. Antalet övergångar till arbete har legat på 630 000 per år de senaste fem åren. AMV:s utgifter under budgetåret 2005 uppgick till ca 67 miljarder kronor[14]. År 2005 omsatte en länsarbetsnämnd i genomsnitt drygt 210 miljoner kronor. I genomsnitt hanterade en arbetsförmedlare ungefär 10 miljoner kronor i olika stöd.

Arbetsförmedlingens Internettjänster har successivt byggts ut. Antalet unika besökare på arbetsförmedlingens webbplats har ökat från ca 700 000 år 2002 till drygt 1,5 miljoner det första kvartalet år 2006. Internet som sökkanal har således ökat kraftigt i betydelse.

---

[12] Uppgifterna i avsnitt 2.1 har om inte annat anges hämtats från AMV:s hemsida och Riksrevisionens rapport 2006:22 Den offentliga arbetsförmedlingen.

[13] Dessa 720 000 olika personer kan ha varit registrerade som arbetslösa allt ifrån en dag till hela året. Det är relativt vanligt att personer som tidigare under året varit arbetslösa och som fått arbete återkommer som arbetslösa.

[14] Kostnader för olika former av försörjningsstöd, dvs. sådana medel som arbetsförmedlingarna inte disponerar till något annat än arbetslösas försörjning, var: a-kassa ungefär 31 miljarder kronor, aktivitetsstöd ungefär 11,5 miljarder kronor, pensionsavgifter för a-kassa och aktivitetsstöd ungefär 4,3 miljarder kronor, lönebidrag ungefär 6,3 miljarder kronor, anställningsstöd ungefär 3,15 miljarder kronor och offentligt skyddat arbete (OSA) ungefär 740 miljoner kronor. (Anställningsstöd och OSA innebär skattekreditering av arbetsgivaren.)

Enligt arbetsordningen för AMS är en av de huvudsakliga uppgifterna för AMS att bistå generaldirektören vid styrningen, ledningen, uppföljningen och utvecklingen av verket samt att ge expertstöd och annat stöd till AMS ledning. AMS utfärdar riktlinjer, ger uppdrag och fördelar resurser mellan länen. Länsarbetsnämnden är länsmyndighet för allmänna arbetsmarknadsfrågor och ansvarar för arbetsförmedlingarna.

De förvaltningsrättsliga föreskrifter som reglerar AMV:s verksamhet är förutom regleringsbrevet och instruktionen (SFS 2001:623) i huvudsak:

- Lag (1976:157) om skyldighet för arbetsgivare att anmäla ledig plats till den offentliga arbetsförmedlingen
- Lag (1997:238) om arbetslöshetsförsäkring
- Lag (1997:239) om arbetslöshetskassor
- Lag (1997:240) om införande av lagen (1997:238) om arbetslöshetsförsäkring och lagen (1997:239) om arbetslöshetskassor
- Lag (2000:625) om arbetsmarknadspolitiska program
- Lag (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.

Relaterat till dessa lagar finns även ett större antal förordningar, bl.a. Förordning (2000:628) om den arbetsmarknadspolitiska verksamheten. Därutöver finns föreskrifter (AMSFS) som AMS har utfärdat.

2.2 Informationstillgångarna och Arbetsmarknadsverkets bedömning av säkerheten för dessa

AMV:s IT-system måste kunna hantera stora penningströmmar och stora volymer integritetskänsliga uppgifter om ett mycket stort antal enskilda personer samt uppgifter om företag och lediga platser.

Enligt AMV besöker dagligen tiotusentals personer och arbetsgivare arbetsförmedlingens webbplats. För att kunna hantera detta tryck på förmedlingarna och förmedla förmedlingens tjänster är inslaget av IT-stöd i AMV:s verksamheter omfattande och verkets IT-beroende är mycket stort.

Det ställs stora krav på att den information som finns i AMV:s informationssystem är säkerställd. Med detta menas att informationens riktighet, tillgänglighet, sekretess samt spårbarhet är skyddad. Felaktiga uppgifter i AMV:s register kan få omfattande konsekvenser. Några exempel på detta är

- att sekretessbelagda personuppgifter röjs,
- att enskild person lider ekonomisk skada då underlag till a-kassa är fel och beslut fattas på felaktiga grunder,

- att statistikunderlag och uppföljningar till bl.a. regering och riksdag blir missvisande,
- att matchning av arbetssökande med arbetsgivarnas lediga platser inte får full effekt på grund av bristfällig registerkvalitet.

Omfattningen av information av stor betydelse för matchningsuppdraget, information till a-kassor och försäkringskassan samt de senare årens utveckling av e-tjänster och exponeringen på Internet, har enligt AMV stor påverkan på AMV:s bedömning av informationssäkerhetens betydelse. Vikten av kontinuitet i verksamheterna är mycket stor, vilket i sin tur ställer höga krav på att IT-systemens förvaltning omgärdas av strikta regelverk vad gäller upprätthållandet av tillgänglighet, riktighet och sekretess.

Utvecklingen av förmedlingsverksamheten går mot att effektivisera förmedlingsarbetet genom att ytterligare utveckla möjligheterna till dialog med hjälp av tekniska lösningar, exempelvis Internet och telefoni. För att detta ska kunna ske på ett tillförlitligt sätt bedömer AMV att det krävs en högre grad av säkerhet, vilket i sin tur kräver mer riktat arbete på att ta fram policydokument och instruktioner för säkerhet samt klassificering av system och information. Ett sådant arbete pågår enligt AMV och är planerat att fortsätta, både på ledningsnivå och inom respektive IT-system.

Enligt Riksrevisionens enkät betraktar AMV informationssäkerheten som en viktig ledningsfråga, vilket också bekräftas av de personer Riksrevisionen intervjuat och av studier av AMV:s styrdokument för IT-säkerheten. Sammantaget bedömer AMV att informationssäkerheten våren 2006 är behäftad med vissa mindre brister. Man bedömer dock att den tekniska säkerheten håller god kvalitet. Myndigheten anger också att informationssäkerheten under en tid inte fått tillräcklig uppmärksamhet från ledningens sida.

AMV:s IT-system finns i Stockholm där driften sker. Totalt finns flera hundra system. Merparten är direkt knutna till AMV:s verksamhetsuppgifter och informationsutbyte mellan interna och externa system. Några av IT-systemen är följande: AIS, ams.se, AFI – självserviceapplikationer på ams.se, Händel, Presto, Åtgärdssystemet, Step samt LedaPlus. Mindre än hälften av systemen är relaterade till AMS:s stödverksamhet (ekonomiadministration, personaladministration, bibliotek, arkiv, resor, samt administration i övrigt) och IT-infrastrukturen, exempelvis olika standardprogram och standardsystem, som förmedlas av IT-enheten vid AMS.

Arbetsmarknadsverkets InformationsSystem – AIS

AIS är den offentliga arbetsförmedlingens interna informationssystem. Det huvudsakliga syftet med AIS är att

- underlätta och stödja det operativa arbetet vid arbetsförmedlingarna med arbetssökande, arbetsgivare, lediga platser och upphandlade utbildningar,
- upprätta information om arbetssökande för att arbetslöshetskassan ska kunna bedöma rätten till ersättning,
- stödja beslutshanteringen vid arbetsförmedlingarna,
- förse eftersystemen (interna och externa) med information för uppföljning, såväl verksamhetsmässig som ekonomisk.

AIS har ca 8 000 dagliga användare. Systemets funktioner är utvecklade för att ge arbetsförmedlarna det administrativa stöd som behövs i deras dagliga arbete. AIS stöder de tre servicevägarna ”Arbetsförmedlingen lokalt”, ”Arbetsförmedlingen Kundtjänst” samt ”Arbetsförmedlingen Internet”.

AIS stöder samtliga verksamhetsprocesser för förmedling av arbete till sökande, och arbetskraft till arbetsgivare (matchning), utbildning (anvisningar och upphandling) och aktivering (anvisning till arbetsmarknadspolitiska program (åtgärdsinsatser)). AIS är också beslutssystemet för insatser/program och fungerar också som diarieföringssystem vad gäller kundärenden[15] (förmedling).

AIS är informationslämnare till interna och externa system, exempelvis:

- Presto (budget och uppföljningssystem),
- Händel (statistikdatabas),
- Åtgärdssystemet (utbetalningssystem),
- STEP (ekonomisystem),
- A-kassa (externt),
- Försäkringskassan (externt).

För ytterligare information om delsystem och särskilda tjänster se bilaga 2.

Arbetsmarknadsverkets webbplats www.ams.se

AMV:s webbplats är en informationskanal för målgrupperna arbetssökande, arbetsgivare samt informationssökande. Webbplatsen delas in i sex huvudområden: söka jobb, rekrytera, yrken/studier, arbetsförmedlingar, nyheter/fakta samt uppgifter om AMV. För ytterligare information om delsystem och särskilda tjänster se bilaga 2.

Självserviceverktyg på www.ams.se – Af Internet (AFI)

På AMV:s webbplats www.ams.se finns de självserviceverktyg (AFI) som används av målgrupperna arbetssökande, arbetsgivare och arbetsförmedlare. Både externa och interna parter utför aktiviteter inom den verksamhet

[15] Övrig diarieföring hanteras av Ärendehanteringssystemet.

AFI stöder. Externa parter utgörs av arbetssökande, arbetsgivare, övriga informationslämnare och informationshämtare, exempelvis press och medborgare. Interna parter utgörs av arbetsförmedlare, redaktörer, informationsproducenter samt informatörer.

AFI består av ett 30-tal publika applikationer i fyra publika portaler samt elva icke publika applikationer i en Handläggarportal. Dessa applikationer fördelas på ams.se mellan huvudområdena *Söka jobb, Rekrytera, Yrken/ studier samt Arbetsförmedlingar.* Från användarsynpunkt uppfattas webbplatsen dock som en och samma portal. Det finns ett antal verksamhetsstöd för att ge preciserade leveranser till målgrupperna i verksamheten från förvaltningsverksamheten. För ytterligare information om delsystem och särskilda tjänster se bilaga 2.

Tillsyn och kontroll över arbetslöshetsförsäkringen

Det finns IT-baserade informationssystem för att bl.a. hålla ett aktuellt register över alla arbetslöshetskassor.

Bidrag som är knutna till AMV:s verksamhet

Olika typer av finansiellt stöd för särskilda aktiviteter överförs via AMV:s transfereringssystem till utbetalande aktörer och vidare till definierade mottagare exempelvis näringsidkare, arbetsgivare, arbetssökande, och handikappade. Stöd till näringsidkare och arbetsgivare utbetalas också av AMV.

Intern revision vid AMS

Det finns IT-baserade informationssystem för att få fram uppgifter till den interna revisionen.

Samverkan med andra myndigheter och externa aktörer

Ett omfattande informationsutbyte sker via IT-baserade informationssystem inom AMV och mellan AMV och externa aktörer såsom Försäkringskassan, Skatteverket, arbetslöshetskassor, Centrala studiestödsnämnden m.fl..

IT-system för verksamhetsutveckling, uppföljning, utvärderingar, prognoser och statistik

Ett flertal stödsystem finns för dessa aktiviteter.

IT-infrastruktur

IT-enheten svarar för den IT-plattform[16] som bygger upp informationssystemen och IT-stödet, exempelvis AIS, AFI, ekonomisystem, informationsutbyte mellan informationssystem inom AMV och mellan externa aktörer, standardiserad uppsättning datorer, standardprogramvaror, standardsystem och kringutrustning vid AMS-enheter och arbetsförmedlingar och länsarbetsnämnder. På några arbetsförmedlingar kan det förekomma persondatorer i särskilda nätverk som inte ingår i IT-enhetens ansvarsområde. Detta kan exempelvis vara persondatorer som är avsedda för arbetssökande, antingen för att skriva arbetsansökan eller för arbetsträning. Dessa har ingen kontakt med AMS nätverk.

[16] Avser den hårdvara (datorer, nätverk och annan utrustning) och mjukvara (programvaror) som utnyttjas men också de resurser i form av kompetens och organisation som behövs för hårdvarans och mjukvarans användning.

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[17] det **engagemang** som ska ägnas informationssäkerhetsfrågorna vid sidan av övriga ledningsuppgifter. Av särskild vikt är att detta görs i sådana myndigheter som har informationstillgångar som är av avgörande betydelse för verksamheten, är sekretessbelagda eller som 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.

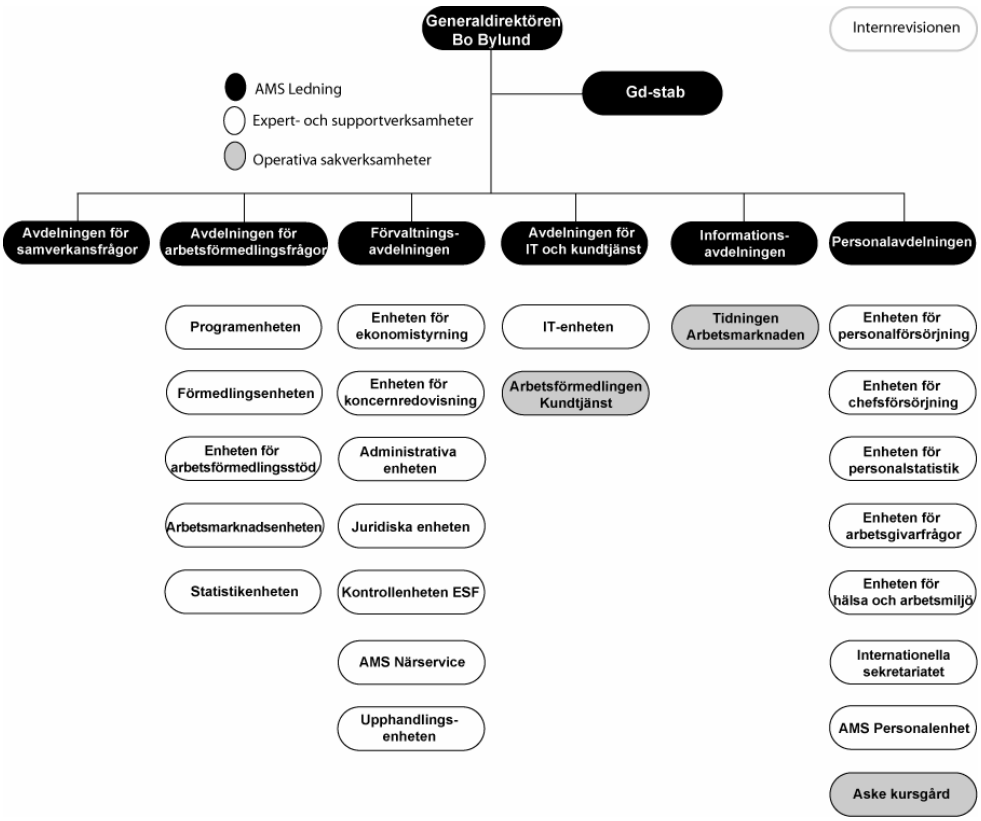
Verksledningen bör tillse att de krav och mål som ska gälla för informationssäkerheten tydligt förmedlas till alla berörda IT-användare inom myndigheten. Detta bör göras i ett sammanhållet övergripande policydokument, en **informationssäkerhetspolicy**. Medarbetarna bör delges vikten av att informationssäkerhetskraven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

3.2 Arbetsmarknadsverkets kontrollmiljö

Följande beskrivning avser förhållandet vid granskningen, dvs. april – juni år 2006. Därefter har vissa organisatoriska förändringar genomförts inom

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

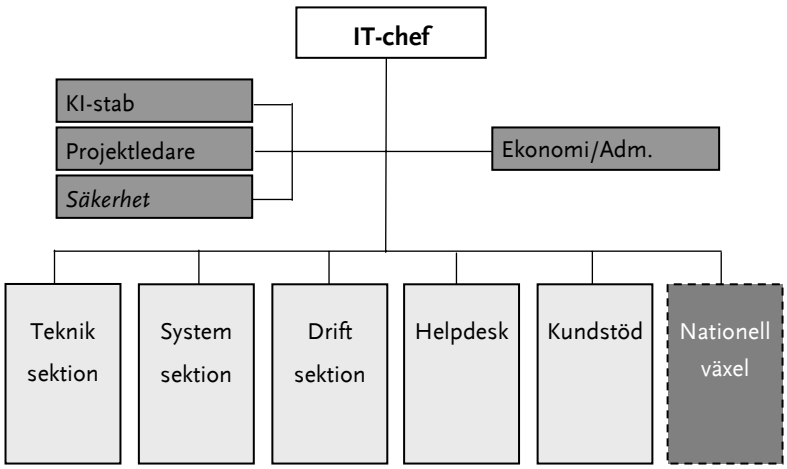
AMV. Säkerhetsarbetet inom AMV är fördelat inom organisationen[18]. Generaldirektören har det övergripande ansvaret för IT-säkerheten inom AMV. I ansvaret ingår att fastställa nödvändiga styrdokument för att uppnå beslutad säkerhetsnivå. Inom AMS finns sex avdelningar. Avdelningsdirektörerna ingår i AMS ledning.



Figur 2: AMS organisation i maj 2006.

Inom Förvaltningsavdelningen finns en säkerhetschef som tillika är säkerhetsskyddschef och ansvarar för samordning av AMV:s säkerhetsarbete. Detta omfattar bl.a. frågor om fredstida krishantering och beredskap, risk- och skadehantering samt säkerhetsfrågor. Ställföreträdande generaldirektören leder avdelningen för IT och kundtjänst (ITKT) med underliggande IT-enheten och Arbetsförmedlingen Kundtjänst.

[18] Arbetsordning för Arbetsmarknadsstyrelsen, IT-säkerhetspolicy för Arbetsmarknadsverket version 1.0, beslutad 2003-04-30.



Figur 3: IT-enhetens organisation i maj 2006.

ITKT ansvarar för bl.a. samordning av strategiska IT-frågor och av AMV:s IT-verksamhet. Ansvaret inbegriper även utformning av policyer, riktlinjer och förvaltning av IT-styrmedel, såsom teknisk plattform, systemägaruppdrag och inriktning av IT-säkerhet, samt ansvar för IT-enheten med uppdrag inom verksamhetsområdet IT. ITKT omfattar också IT-staben med tre personer, varav en är IT-säkerhetssamordnare.

I övrigt följer säkerhetsansvaret den fastställda ansvars- och beslutsordningen för linjeorganisationen. Var och en, som är ansvarig för någon del av verksamheten, ansvarar också för IT-säkerheten inom sitt område. Varje medarbetare är skyldig att följa de regler som beslutats för IT-säkerheten genom att ta del av och följa de säkerhetsregler som finns för de IT-system som den enskilde användaren har behörighet till.

AMV har upprättat ett antal styrdokument för IT-verksamheten. Det övergripande centrala dokumentet är en **IT-säkerhetspolicy (april 2003)**. I IT-säkerhetspolicyn definierar ledningen grunden för valt ledningssystem, mål, organisation, roller och ansvar för IT-säkerhetsarbetet, krav på risk- och sårbarhetsanalys, viktiga kontrollfunktioner, utbildning samt uppföljning och rapportering.

AMS arbetsordning och IT-säkerhetspolicyn utgör de formella **förutsättningar** som ledningen skapat för hur säkerhetsarbetet ska bedrivas och organiseras vad gäller ansvar och uppföljning.

Av IT-säkerhetspolicyn framgår att AMV har valt att organisera arbetet med IT-säkerhet utifrån dåvarande Överstyrelsen för civil beredskaps (ÖCB) norm om grundsäkerhet för samhällsviktiga datasystem (FA22[19]). FA22 har

[19] Enligt beredskapsförordningen (1993:242) ställdes krav på de myndigheter som ska följa säkerhetskraven för tekniska IT-system för att kunna utföra sitt arbete. ÖCB gav ut Föreskrifter om grundsäkerhet för samhällsviktiga datasystem hos beredskapsmyndigheter (1998:1). I syfte att förtydliga detta föreskrev ÖCB allmänna råd som benämns FA22 (Föreskrifter och Allmänna råd till beredskapsförordningen § 22 a).

dock upphört att gälla. KBM, som delvis har tagit över ÖCB:s uppgifter, har i stället tagit fram en rekommendation för basnivå för informationssäkerhet (BITS[20]). Inom AMV pågår sedan våren 2006 ett arbete med att revidera policydokument för att införa BITS.

FA22 innebär att fokus läggs på enskilda IT-system och att det i första hand är systemägarna som ansvarar för IT-säkerheten. BITS utvidgar säkerhetsbegreppet från IT-säkerhet till informationssäkerhet, och säkerhetsarbetet från att gälla IT-system till att gälla informationssystem[21]. I BITS, till skillnad från i FA22, betonas samtidigt ledningens engagemang och ledningens behov av samordning av informationssäkerhetsarbetet mellan den operativa nivån och ledningen. (Se även bilaga 1 avseende skillnader mellan FA22 och BITS.)

IT-säkerhetspolicyn beslutades den 30 april 2003 efter att AMV:s styrelse hade efterfrågat en IT-säkerhetspolicy. Enligt policyn är den generaldirektörens övergripande styrdokument för att uppnå god kvalitet och enhetlighet i IT-säkerhetsarbetet. Av IT-säkerhetspolicyn framgår att ”för att möta kraven i FA22 samt för att uppnå en kvalitativ och effektiv IT-säkerhet, kommer AMV att utarbeta och fastställa tre myndighetsövergripande dokument. Dessa dokument är IT-säkerhetspolicy för AMV med bilagor, generella riktlinjer för AMV:s IT-säkerhetsarbete samt AMV:s IT-säkerhetsinstruktion”.

I IT-säkerhetspolicyn fastställer generaldirektören följande roller och ansvarsområden:

- *IT-direktören*, som är ställföreträdande generaldirektören, svarar för att IT-säkerhetspolicyn uppdateras samt för att utarbeta ”Generella riktlinjer för IT-säkerhetsarbetet”.
- *IT-ansvarig,* som är chefen för IT-enheten, ska utarbeta direkta och praktiska instruktioner, ansvara för den operativa IT-säkerheten och att de tekniska delarna i AMV:s IT-system fungerar samt informera IT-säkerhetssamordnaren då oförenliga IT-säkerhetsfrågor uppstår.
- *IT-säkerhetssamordnaren,* som är organisatoriskt placerad i IT-staben och direkt underställd IT-direktören i säkerhetsfrågor, ska stödja systemägare och IT-ansvarig i arbetet med att uppnå IT-säkerhetspolicyns mål. IT-säkerhetssamordnaren ska utarbeta riktlinjer för hur risk- och sårbarhetsanalyser ska genomföras. Systemägare och verksamhetsansvariga väljer dock själva på vilket sätt och med vilka resurser de vill uppnå målen. Samordnaren har ett aktivt uppföljningsansvar för IT-säkerhetsarbetet. Uppföljning och åtgärdsförslag ska rapporteras av IT-säkerhetssamordnaren direkt till IT-direktören.

---

[20] Basnivå för informationssäkerhet, Krisberedskapsmyndigheten 2006:1.

[21] Därmed menas främst att även annan information än den som behandlas med IT ska omfattas av säkerhetsarbetet.

- *Systemägarna,* som ofta är avdelnings- eller enhetschefer, har det dagliga ansvaret för att policy och riktlinjer följs och för att följa upp att användarna följer IT-säkerhetskraven.
- *Varje chef* är ansvarig för att policy och riktlinjer efterlevs i verksamheten samt för att medarbetare har tillräcklig kompetens.
- En *IT-ledningsgrupp* ska finnas, ledd av IT-direktören och bestående av samtliga systemägare, IT-ansvarig, IT-staben och de centrala fackliga organisationerna. Gruppen ska diskutera verksamhetsövergripande IT-frågor och vara ett remissorgan till IT-direktören innan denne fattar beslut i verksövergripande IT-frågor.
- En *beredningsgrupp* ska finnas, ledd av IT-stabschefen och bemannad med samtliga systemförvaltare och IT-ansvarig. Gruppen ska vara ett stöd till IT-ledningsgruppen i deras ställningstaganden.

Enligt IT-säkerhetspolicyn ska även följande finnas:

- *Systemsäkerhetsplaner* för varje verksamhetskritiskt IT-system. Dessa ska innehålla de samlade kraven på säkerhet – grundkrav och tilläggskrav – som ställs på systemet. I respektive plan, som fastställs av systemägaren, anges krav på tillgänglighet, tillförlitlighet, sekretess och spårbarhet för systemet i fråga.
- *Incidenthantering*, vilket omfattar såväl att hantera de tillfällen då incidenter inträffar som att ha en väl fungerande incidenthantering för att samla kunskap och bygga upp skydd mot framtida risker och hot.
- *Risk- och sårbarhetsanalyser*. Dessa ska kontinuerligt genomföras av systemägare och IT-ansvarig.
- *Uppföljning och rapportering.* Kraven på att AMV:s informationshantering är uppfyllda ska kontinuerligt följas upp. Avvikelser eller avsteg ska rapporteras till IT-direktören. Juridiska enheten har ansvaret för att följa upp att AMV följer de lagar, förordningar och riktlinjer som är aktuella.
- *Utbildning i IT-säkerhet*. Genom utbildningar och/eller riktade informationssatsningar ska samtliga medarbetare ges kunskap om AMV:s övergripande styrdokument för IT-säkerhetsarbetet.

3.3 Iakttagelser

Granskningen under våren 2006 visar att ledningen inte har sett till att flera väsentliga delar i den gällande IT-säkerhetspolicyn från år 2003 har genomförts. De generella riktlinjer för AMV:s IT-säkerhetsarbete samt AMV:s IT-säkerhetsinstruktion som ska finnas enligt policyn har inte tagits fram.

Det finns ingen dokumentation som visar hur ledningen ska agera om besluten i IT-säkerhetspolicyn inte genomförs.

Av ITKT:s verksamhetsplan för år 2006 framgår att IT-säkerhetsarbetet på övergripande nivå har legat stilla under år 2005 och att IT-säkerhetspolicyn behöver uppdateras och fördjupas samt kommuniceras till samtliga medarbetare. I planen sägs att det krävs utformning av riktlinjer och instruktioner för att operationalisera IT-säkerhetspolicyn. Vidare anges att det behövs ett utbildningsmaterial och ett antal konferenser/möten för att kommunicera policyn till medarbetarna.

Enligt IT-säkerhetspolicyn ansvarar IT-direktören för att policyn hålls uppdaterad och IT-säkerhetssamordnaren för att utarbeta förslag till IT-säkerhetspolicy. Det framgår inte av IT-säkerhetspolicyn om IT-säkerhetssamordnaren har mandat att genomföra besluten i policyn. Det saknas även specifika anvisningar för samordnarens arbete med IT-säkerheten.

Ett arbete med att revidera IT-säkerhetspolicyn påbörjades under våren 2006. IT-enheten inledde arbetet efter att en konsult som IT-enheten anlitat under år 2005 påtalat ett behov av att förstärka IT-säkerheten. I en intervju framhåller IT-ansvarig att komplexiteten i IT-miljön har ökat under senare år, vilket ställer större krav på säkerhetsarbetet. Den IT-ansvarige inrättade därför en säkerhetsstab inom IT-enheten. Säkerhetsstaben fick i uppgift att uppdatera IT-säkerhetspolicyn. Det är dock IT-säkerhetssamordnaren vid IT-staben som formellt ansvarar för att utarbeta förslag till IT-säkerhetspolicy och denne har därför övertagit ansvaret för arbetet. IT-staben och IT-enheten samarbetar nu i revideringsarbetet.

I dag finns ingen samordningsorganisation för IT-frågor. Den IT-ledningsgrupp och beredningsgrupp för IT-frågor som beslutades i IT-säkerhetspolicyn upphörde för två till tre år sedan efter överväganden av dåvarande IT-direktören. Generaldirektören har dock inte fattat något formellt beslut i frågan. IT-frågor behandlas i dag, liksom övriga större frågor, i den s.k. GD-beredningen. Flera av de personer som Riksrevisionen har intervjuat uttrycker ett behov av en särskild samordningsorganisation för IT-frågor, och i vissa fall har i stället andra samordningsaktiviteter uppstått. En annan uppfattning är att det är tillräckligt med GD-beredningen eftersom generaldirektören ändå måste fatta beslut om alla större frågor. Ytterligare ett argument för denna uppfattning som förs fram är att AMV nu dessutom har en modell för systemförvaltning[22], vilket ger viss möjlighet till samordning av förvaltningsarbetet.

Arbetet med att etablera och införa modellen för systemförvaltning har bedrivits sedan år 2002 och inledningsvis parallellt med arbetet med IT-säkerhetspolicyn. Vid granskningen pågick ett arbete med att utarbeta en

[22] Modell för systemförvaltning inom AMV v 1.1, beslutad 2004-05-27.

ny version av förvaltningsmodellen. Även om inledningsvis en viss samordning gjordes av de två styrdokumenten kvarstår ett behov av ytterligare samordning, bl.a. av vissa viktiga begrepp. Ett sådant arbete med samordning pågår enligt uppgift från AMV.

Flera av de övriga funktioner och säkerhetsåtgärder som beslutats i IT-säkerhetspolicyn, som exempel systemsäkerhetsplaner, har inte genomförts fullt ut. Det saknas även beslut om vilka system som är verksamhetskritiska samt en dokumenterad rutin för incidentrapportering. Det finns inte heller dokumenterat att ledningen har följt upp dessa brister och agerat för att besluten ska genomföras. Riksrevisionen återkommer till detta i kapitlen 4 och 5.

I styrdokumenten har inte utpekats något ansvar för att genomföra och sammanställa en samlad riskanalys som kan ge ledningen en samlad bild av IT-säkerhetsarbetet för hela AMV. Ledningen har sedan IT-säkerhetspolicyn beslutades inte agerat för att risk- och sårbarhetsanalyser faktiskt ska göras för samtliga system. Riskanalyser behandlas vidare i kapitel 4.

Ledningens uppföljning av att säkerhetsarbetet genomförs i enlighet med IT-säkerhetspolicyn är en viktig del av säkerhetsarbetet. Inom AMV har ansvaret för säkerheten, i enlighet med principerna i ÖCB:s FA22, till stor del delegerats ned i organisationen, till systemägarna. Enligt IT-säkerhetspolicyn ska IT-säkerhetssamordnaren rapportera uppföljning och åtgärdsförslag till IT-direktören. Det preciseras dock inte i policyn eller i något annat dokument hur detta ska göras. Det finns inte heller i något styrdokument beskrivet hur rapporteringen från IT-direktören till de övriga i ledningen ska ske för att dessa ska få information om hur säkerhetsarbetet genomförs. Riksrevisionen har uppmärksammat att det råder oklarhet inom organisationen om vem eller vilka på ledningsnivå som ansvarar för att följa upp att IT-säkerhetsarbetet fungerar i enlighet med IT-säkerhetspolicyn. I intervjuer har olika uppfattningar framkommit om huruvida det är IT-direktörens eller linjechefernas ansvar att se till att en uppföljning görs.

Juridiska enheten har enligt IT-säkerhetspolicyn ansvaret för att följa upp att AMV följer de lagar, förordningar och riktlinjer som är aktuella. Enligt verksjuristens arbetsordning har denne dock inte ansvar för att följa upp informationssäkerhetsåtgärder med koppling till exempelvis personuppgiftslagen och sekretesslagen samt hantering av dokument i IT-systemen.

Riksrevisionen konstaterar att det inte finns en dokumenterad regelbunden, systematisk uppföljning från verksledningens sida av säkerhetsarbetet och av att beslutade åtgärder vidtas.

Utöver beslutade styrdokument saknas i stort sett dokument som visar att ledningen har ett **engagemang** i informationssäkerhetsfrågor. Det finns inte heller fastställda rutiner för att diskutera IT-frågor i ledningsgruppen. Riksrevisionen har efterfrågat och fått protokoll från lednings- och styrelse-

möten, som visar att informationssäkerhetsfrågor inte har diskuterats. Det finns inte heller dokumentation som visar att styrelsen eller ledningen har följt upp att IT-säkerhetspolicyn från år 2003 implementerats, eller efterfrågat de riktlinjer och instruktioner som enligt policyn ska tas fram.

Beträffande ledningens **förtrogenhet** med informationssäkerhetsarbetets ledningsfrågor kan konstateras att ledningsgruppen inte genomgått någon utbildning i dessa frågor (se kapitel 6).

3.4 Bedömning

Det faktum att de styrdokument – riktlinjer och instruktioner – som beslutats i IT-säkerhetspolicyn, och som ansetts nödvändiga för det fortsatta IT-säkerhetsarbetet, inte har tagits fram visar enligt Riksrevisionens bedömning att ledningen inte i tillräcklig utsträckning har styrt IT-säkerhetsarbetet och följt upp att detta sker i enlighet med den beslutade policyn.

Frånvaron av en övergripande riskhanteringsprocess, uppföljning och riskanalyser minskar enligt Riksrevisionens bedömning ledningens förutsättningar att göra en väl underbyggd prioritering av åtgärder utifrån ett helhetsperspektiv så att beslutad säkerhetsnivå uppnås. Att ledningen inte efterfrågat samlade riskanalyser eller en dokumenterad rutin för incidentrapportering bidrar till Riksrevisionens intryck av brister i ledningens engagemang i informationssäkerhetsfrågorna.

Genom att ledningen har infört ett ledningssystem för informationssäkerhet som bygger på FA22, betonas systemägarnas ansvar framför ledningens respektive IT-säkerhetssamordnarens ansvar för organisationens IT-säkerhetsarbete. Riksrevisionens bedömning är att eftersom systemägarna har ett jämförelsevis stort ansvar riskerar samordnarens funktion att komma i bakgrunden i förhållande till systemägarnas funktion. En reducerad samordningsfunktion, ett otydligt mandat för samordnaren och oklara rutiner för rapportering från samordningsnivån och uppåt i organisationen medför att IT-säkerhetssamordnaren får begränsade möjligheter att utöva sin roll på det sätt som avsetts. Dessa förhållanden kan till viss del förklara de svårigheter som finns i den organisation som ledningen valt för sitt informationssäkerhetsarbete.

Förhållandet att grundläggande styrdokument som IT-säkerhetspolicyn och systemförvaltningsmodellen inte är samstämmiga beträffande viktiga begrepp leder enligt Riksrevisionens bedömning till en osäkerhet i organisationen och visar att ledningen inte på ett tydligt sätt har styrt AMV:s informationssäkerhetsarbete. Att ledningsgruppen inte har genomgått någon specifik utbildning för att skaffa sig kunskap om informationssäkerhetsarbetets

ledningsfrågor medför risk för brister i ledningens beslut avseende informationssäkerhetsarbetet.

De brister som beskrivits ovan innebär att säkerhetsarbetet inte bedrivs på ett enhetligt sätt inom AMV och inte heller i enlighet med ledningens intentioner. Det finns även risk för att åtgärder inte vidtas i tillräcklig utsträckning för att förebygga och begränsa konsekvenser av hot och störningar i AMV:s IT-stöd.

Riksrevisionen bedömer därför sammantaget att ledningens kontrollmiljö när det gäller informationssäkerhet har brister som främst rör förutsättningarna för informationssäkerhetsarbetet samt ledningens engagemang för detta arbete. Dessa brister har försvårat kommunikation och samverkan mellan olika aktörer i informationssäkerhetsarbetet och har medfört att vissa beslutade säkerhetsåtgärder inte har införts fullt ut, vilket påverkar AMV:s informationssäkerhet negativt.

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 hot som realiserats. För att bedöma om en verksamhet har genomfört en adekvat riskanalys har Riksrevisionen använt följande sex kriterier.

Som underlag för analysen bör de skyddsvärda informationstillgångarna identifieras[23]. 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**[24]. Riskanalysen bör uppdateras årligen, och däremellan vid behov.

Analysen bör omfatta **alla typer av 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 säkerhetsåtgärder[25] 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 begränsa dem i framtiden. Incidenter bör systematiskt dokumenteras och

---

[23] Identifieringen bör omfatta vilka de är, vem som är ägare/har ansvar för dem, var de finns samt vilka beroenden som finns mellan olika informationstillgångar.

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

[25] 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.

rapporteras så att en bild av de upptäckta säkerhetsproblem som finns i myndighetens informationshantering kan skapas.

4.2 Bakgrund till Arbetsmarknadsverkets arbete med riskanalyser

Regeringen gav i början av 2000-talet dåvarande ÖCB i uppdrag att genomföra en bedömning av i vilken utsträckning olika myndigheter levde upp till kraven på grundsäkerhet i samhällsviktiga IT-system. Som ett led i detta arbete behandlades hos AMS frågan om risk- och sårbarhetsanalyser av AMV:s IT-miljö i en särskild intern promemoria[26] i början av år 2001. I promemorian redovisar AMS att myndigheten vid ingången av år 2001 inte hade ett strukturerat angreppssätt för arbetet med riskanalyser inom IT-området. Dåvarande IT-staben såg det som angeläget att fastställa formerna för detta arbete. I promemorian beslutades därför om krav på att systemägarna och IT-enheten skulle genomföra risk- och sårbarhetsanalyser enligt en tidplan och att rapportering skulle ske till IT-stab. Högsta prioritet gällde analyserna av de öppna systemen på Internet och AIS. Av promemorian framgår att ÖCB:s metod FA22 skulle användas och att riskanalyser skulle göras regelbundet.

AMV återkom två år senare i IT-säkerhetspolicyn (april 2003) om hur arbetet med analys av informationssäkerhetsrisker ska organiseras. Av policyn framgår:

- Säkerhetsansvaret följer den fastställda *ansvars- och beslutsordningen* för linjeorganisationen. Inom ramen för resurstilldelningen fattar systemägaren de avgörande besluten om det egna IT-systemet.
- All information ska *informations- och säkerhetsklassas*. Denna princip gäller även elektronisk information. Det är informationsägaren[27] i samverkan med systemägaren som beslutar om informationens säkerhetsklassning.
- Det ska finnas en väl fungerande *incidentrapportering* för att samla kunskap och bygga upp skydd mot framtida risker och hot. IT-säkerhetssamordnaren ska samordna incidentrapporteringen. Personalen ska rapportera IT-incidenter som de upptäcker i sin tjänsteutövning till Helpdesk inom IT-enheten. Den IT-ansvarige ska vidare övervaka och rapportera IT-incidenter till IT-säkerhetssamordnaren samt föreslå lösningar för att upprätthålla en hög IT-säkerhet.

[26] Risk- och sårbarhetsanalys av AMV:s IT-miljö, beslutad 2001-02-06, dnr (VLK) 01-000718-06.

[27] Enligt AMV:s IT-säkerhetspolicy är informationsägare primärt den tjänsteman inom AMV som först skapar och registrerar information i AMV:s IT-system. Informationsägare kan även vara den som ansvarar för kvaliteten av informationen i AMV:s IT-system.

- IT-säkerhetssamordnaren utarbetar *metoder* och riktlinjer, för hur riskanalyser ska genomföras.
- Systemägare respektive IT-ansvarig ska kontinuerligt genomföra *risk- och sårbarhetsanalyser.* I detta ligger att bedöma säkerhetskraven när det gäller tillgänglighet, tillförlitlighet, sekretess och spårbarhet. Resultaten av dessa analyser ska dokumenteras (i en systemsäkerhetsplan) och rapporteras till IT-direktören och till IT-ledningsgruppen. IT-säkerhetssamordnaren ska biträda systemägarna för att ta fram systemsäkerhetsplaner.
- Systemägaren ska i systemsäkerhetsplanen besluta om säkerhetsnivån. I detta ligger bl.a. att fastställa hotbilden, utifrån risk- och sårbarhetsanalyserna, för systemet. Systemägare och/eller verksamhetsansvariga ska välja vilka *åtgärder* och med vilka resurser de vill uppnå uppställda mål. Systemägaren ska formellt driftgodkänna systemet utifrån beslutade krav.
- Samtliga verksamhetskritiska IT-system ska senast 2004-12-31 ha uppnått *grundsäkerhet* enligt FA22 (se kapitel 3 om FA22).

4.3 Iakttagelser

Arbetet med riskanalyser inom AMV är inte i tillräcklig utsträckning **organiserat** i enlighet med dels AMV:s egna krav, dels Riksrevisionens bedömningsgrund. Detta framgår i det följande.

AMV anger i Riksrevisionens enkät att det finns en aktuell sammanställning över myndighetens informationstillgångar. Den **förteckning** som användes vid granskningstillfället togs fram inför millennieskiftet år 2000. Det finns inte någon dokumenterad rutin för att underhålla förteckningen och vissa uppgifter är inte aktuella. I en intervju framför IT-enheten behov av en mer aktuell förteckning.

Vissa krav i Riksrevisionens bedömningsgrund för informationstillgångar uppfylls inte heller av AMV:s förteckning, exempelvis uppgifter om databaser, system- och driftdokumentation och programlicenser. Vidare är inte hoten, genomförda säkerhetsåtgärder och kvarstående sårbarheter per objekt dokumenterade. Det framgår av intervjuer att begreppen i förteckningen inte är samordnade med begreppen i AMV:s modell för systemförvaltning (se även kapitel 3).

Av svaret på Riksrevisionens enkät framgår att AMV inte **säkerhetsklassificerar sina informationstillgångar**, men att detta planeras ske framöver. Riksrevisionen konstaterar att detta inte är i linje med IT-säkerhetspolicyn från år 2003 där ledningen anger att informationen ska säkerhetsklassas. Dokumentstudien visar vidare att det inte finns ledningsbeslut om vilka

IT-system som är verksamhetskritiska. Av intervjuer framkommer att det inom AMV ändå finns en uppfattning om vilka system som är mest kritiska. IT-enheten å sin sida för fram att enheten behöver veta vilka system som är verksamhetskritiska som underlag för säkerhetsinsatser. IT-staben anser att det bör räcka med att klassa informationen som öppen och allmän, eller skyddad. I praktiken har systemägarna själva, och inte ledningsnivån, fått bedöma om systemen är verksamhetskritiska eller inte. Detta görs dock utan något gemensamt stöd och utan formell dokumentation. Det är även oklart vilken roll som informationsägarna har i informationsklassningen. Av intervjuer framgår att AMV har testat en modell för säkerhetsklassning. Metoden ansågs fungera, men frågan har inte tagits upp i ledningen för beslut.

Enligt IT-säkerhetspolicyn ska hantering och rapportering av **incidenter** regleras i de generella riktlinjerna och IT-säkerhetsinstruktionen. IT-staben har tagit fram utkast till riktlinjer för incidentrapportering, men något beslut har inte fattats och därmed finns ingen formell rapporteringsrutin införd.

Incidentrapporteringen inom AMV följer den organisatoriska indelningen från systemägare via linjechef och avdelningschef till ledningen. Den IT-ansvarige informerar IT-direktören, men också säkerhetschef samt berörda systemägare. På eget initiativ utbyter vissa systemförvaltare sinsemellan incidentinformation. Användare av IT-systemen rapporterar tekniska incidenter till en så kallad Helpdesk. Dessa sammanställs och dokumenteras, vilket har gjort det möjligt att åtgärda generella användarfel. Länsarbetsnämnderna har rutiner för att rapportera incidenter till säkerhetschef respektive Helpdesk.

Information från verksamheterna om incidenter rapporteras inte systematiskt till IT-staben för en samlad analys, rapportering till ledningen och återkoppling till verksamheterna. Enligt IT-enheten har AMV:s IT-system hittills varit utsatt för mycket få incidenter som kommit till IT-enhetens kännedom. Av intervjuer framgår dock en osäkerhet om alla incidenter rapporteras.

Ledningens uppföljning av IT-säkerhetsarbetet utgörs främst av en händelsestyrd avrapportering som begränsas till allvarligare incidenter.

I Riksrevisionens enkät anger AMV att det finns en dokumenterad och tillämpad **process för risk- och sårbarhetsanalyser**. Av intervjuer framkommer dock att det inte finns någon gemensam, beslutad uppsättning **metoder** för analys av olika typer av risker i syfte att styra kvalitet och jämförbarhet i riskanalyserna.

AMV har genomfört ett utvecklingsprojekt för att få fram en gemensam riskanalysmodell för IT-systemen. Utvecklingsarbetet syftade till att bli

grunden för regelbundna riskanalyser av AIS[28] och ams.se. Av intervjuer framgår att regelbundna analyser ännu inte görs. Modellen har inte heller överförts till systemägare och systemförvaltare för andra system.[29]

På avdelningsnivå görs, enligt intervju, bedömningen att de riskanalyser som görs per system, utan att analyserna stöds av beslutade gemensamma metoder, ändå får fram vad som är kritiskt att åtgärda per system.

Inom Förvaltningsavdelningen vid AMS pågår hösten 2006 ett arbete med att utveckla och införa ett IT-baserat risk- och sårbarhetsanalysverktyg för säkerhetsfrågor i allmänhet. Av en intervju framgår att i detta arbete kommer möjligheten att beaktas att välja ett IT-verktyg som även skulle kunna uppfylla krav på stöd för risk- och sårbarhetsanalyser för IT-systemen.

Riksrevisionen har översiktligt studerat förekomsten av risk- och sårbarhetsanalys för informationssäkerheten vid två länsarbetsnämnder. Generaldirektören har regelbundna länsgenomgångar, men frågor om informationssäkerhet ingår inte. Länsarbetsnämnden och arbetsförmedlingen genomför risk- och säkerhetsanalyser, på uppdrag av säkerhetschefen, enligt en standardiserad mall[30]. Dessa analyser omfattar främst andra områden än informationssäkerhet. Ett fåtal frågor rör IT-säkerheten. Rapporteringen av riskanalysen görs till såväl länsarbetsnämnden som AMS (säkerhetschefen).

Enligt intervjuer har systemägarna under senare år inte skickat dokumenterade risk- och sårbarhetsanalyser för IT-systemen till IT-direktören eller IT-ledningsgruppen, vilket ska göras enligt IT-säkerhetspolicyn[31]. Det finns inte heller några dokument som visar att brister per system upptäckta i arbetet med riskanalyserna har förts vidare från IT-staben och IT-direktören till ledningen på ett systematiskt sätt. Ledningen har å sin sida inte följt upp riskanalysarbetet på systemnivå. Ansvaret för att få fram årliga riskanalyser ligger hos IT-direktören.

Riksrevisionen konstaterar att nuvarande generaldirektör har en ambition att verksamhetsansvariga ska göra årliga riskanalyser, genom att använda en gemensam metod, som gör det möjligt att bedöma samlade risker och behov av säkerhetsåtgärder. Denna bedömning kan sedan presenteras för styrelsen.

Under intervjuerna har det framkommit exempel på att **alla typer av risker** inte behandlas tillfredsställande i AMV:s riskanalyser. Interna risker, exempelvis att personal utför oönskade handlingar i informationssystemen,

---

[28] Avsikten var att göra riskanalysen för hela AIS. Hittills har en riskanalys gjorts för delsystemet AIS-Å.

[29] Det finns riskanalysrapporter som avser enskilda IT-system, men dessa analyser har tagits fram med annan metod.

[30] Mall för riskidentifiering och riskanalys som Länsarbetsnämnden Stockholm överlämnat.

[31] IT-säkerhetspolicyn avsnitten 7.5 och 19.

övervägs inte. Utgångspunkten för ledning och verksamhetschefer är att de litar på sin personal.

Av intervjuer med personer på länsarbetsnämnden framgår att det förekommer att personal vid arbetsförmedlingen registrerar information om en arbetssökande på fel person, främst beroende på att systemen inte varit tillräckligt användaranpassade.

En allvarlig incident inträffade sent år 2005. Externa användare av ams.se utgick från att de arbetade med egna data i systemet, men i några fall drabbades andra användare av de ändringar av data som gjordes. Inloggningstjänsten till ams.se stängdes i två veckor, vilket minskade möjligheterna bl.a. till matchning mellan arbetssökande och arbetsgivare. En liknande incident inträffade i juni 2006 då en ny systemversion av ams.se innehöll fel som medförde att hela webbsidan på Internet inte blev tillgänglig. I båda fallen uppstod incidenterna efter att en ny levererad systemversion gick i drift.

Granskningen visar att det inom AMV inte finns någon utsedd person med ansvar för att ta fram och ge ledningen en samlad övergripande bild av risker och hot mot IT-systemen och verksamheterna. Av intervjuer framgår att ledningen tidigare inte har efterfrågat någon samlad riskanalys.

Enligt ledningens beslut är ett krav att **åtgärdsplaner** för IT-säkerhetsarbetet ska finnas för verksamhetskritiska system, men helst för samtliga system. Granskningen visar att det inte finns sådana åtgärdsplaner för samtliga system och som följd av detta inte heller en samlad åtgärdsplan för hela myndigheten. Även internrevisionen vid AMV har i sina granskningsrapporter[32] tagit upp problemet med att det saknas fastställda och dokumenterade säkerhetsmässiga bedömningar för flera system inom AMV. Bilden av vilka åtgärder som är nödvändiga är således ofullständig. På ledningsnivå är man medveten om att det finns behov av att analysera beroendeförhållanden mellan system som grund för diskussioner om åtgärder för att säkra systemsamband.

I samband med att systemsäkerhetsplaner togs fram för AIS och ams.se dokumenterades ett antal säkerhetsbrister som inte kunde hanteras inom systemens förvaltningsverksamhet. Promemorian[33] från juni år 2005 överlämnades till berörda chefer och IT-säkerhetssamordnare. Enligt intervjuer har ledningen inte fattat beslut om de föreslagna åtgärderna. Det finns även ytterligare åtgärder enligt systemsäkerhetsplanen för ams.se som inte har vidtagits. Detta beror enligt intervjuer på att de föreslagna åtgärderna bör genomföras först i samband med att ett gemensamt förmedlingssystem införs. Ett sådant nytt system har planerats, men skjutits upp under flera år.

---

[32] Granskning av behörighetsadministration och behörighetskontroller för handläggarsystemet AIS (AMS Internrevisionen Revisionsrapport nr 1:18/05, 2006-01-12).

[33] IT-säkerhetsarbete 2004-2005 på Af-system, PM 2005-06-03.

Beslut om åtgärder för IT-säkerheten fattas i den årliga verksamhetsplanerings- och budgetprocessen. En genomgång sker av samtliga system och utvecklingsprojekt[34] som är aktuella. På ledningsnivå påpekas att detta är en grov prioritering. Några uttryckliga mål för de enskilda verksamheterna till vilka informationssäkerhetsrisker och åtgärder kan kopplas som grund för prioriteringar har dock inte framkommit i granskningen.

Prioriteringar av enskilda säkerhetsåtgärder mellan system görs i första hand inom respektive avdelning. Fördelningen av medel för informationssäkerhet mellan avdelningar bygger således inte på ledningens prioriteringar från övergripande nivå. Det finns inte någon sammanställning över kostnaderna för de säkerhetsinvesteringar som görs. En konsekvens av detta är att det inte finns någon samlad bild över behovet av säkerhetsåtgärder och säkerhetsinvesteringar i IT-systemen och inte heller någon samlad åtgärdsplan.

Det finns inga dokument som visar att ledningen följt upp att de säkerhetsåtgärder som har prioriterats och beslutats i verksamhetsplaneringen och budgetprocessen för respektive system har genomförts och fungerar som avsett. Internrevisionen gjorde en uppföljande granskning[35] år 2005 av sina rekommendationer till åtgärder från en systemgranskning år 2002. Resultatet från uppföljningen visade att vissa åtgärder hade vidtagits medan andra inte hade påbörjats.

4.4 Bedömning

Riksrevisionens bedömning är att ledningen för AMV inte fullt ut har lyckats genomföra sitt beslut om hur arbetet med riskanalyser ska utföras på systemnivå. Det finns inget ledningsbeslut om att riskanalyser ska analyseras och sammanställas på övergripande nivå. Detta medför enligt Riksrevisionens bedömning att ledningen inte får en överblick av riskerna inom AMV och inte heller har möjlighet att upprätta en samlad åtgärdsplan. Därmed finns risk att analyserna och de valda säkerhetsåtgärderna på systemnivå inte är tillräckligt välgrundade för att ge en god informationssäkerhet. Allvarliga incidenter som inträffat i samband med byten av systemversioner pekar på svagheter i riskanalyserna av behovet av kontinuitetsplaner vid versionsbyten.

---

[34] Generaldirektören har utsett en person att administrera en ”projektportfölj”. I ansvaret ligger att samråda med de projekt som pågår. När ett projekt gör en prioritering måste samordning ske med andra berörda projekt. Ett projekt kan vid behov initiera en åtgärd i ett annat projekt eller förvaltningsobjekt.

[35] Granskning av behörighetsadministration och behörighetskontroller för handläggarsystemet AIS (AMS Internrevisionen Revisionsrapport nr 1:18/05, 2006-01-12).

Ledningen kan inte heller överblicka utestående[36] risker och hur hanteringen av dessa utvecklas över tiden. Riksrevisionen bedömer att ledningen därmed har en begränsad medvetenhet om riskerna.

[36] Med utestående risker avses risker som ledningen medvetet valt att inte skydda AMV för. Bakgrunden kan vara att skyddskostnaderna anses för höga eller incidenter alltför osannolika.

5 Ledningens kontrollfunktioner och säkerhetsåtgärder

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 samt tekniska säkerhetsåtgärder såsom behörighetskontroller och loggningsförfaranden. Kontrollfunktionerna utgör sammantagna en väsentlig del av myndighetens ledningssystem för informationssäkerhet.

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

Ett ledningssystem för informationssäkerhet bör normalt ha följande **omfattning** när det gäller komponenter[37]:

- 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[38],
- process för säkerhetskopiering av all verksamhetskritisk information,

[37] 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.

[38] Policy som reglerar åtkomst till informationstillgångar.

- process för styrning av utveckling och förändringar i IT-miljö, IT-system och bemanning,
- tekniska säkerhetsåtgärder exempelvis behörighetskontrollsystem, virusskydd, och brandväggar,
- 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[39] i informationssäkerhetsarbetet och hur ansvar och befogenheter för myndighetens informationssäkerhet fördelats på dessa,
- processer för återkommande uppföljning och förvaltning av ledningssystemet.

Komponenterna bör vara utformade utifrån myndighetens särskilda behov och därvid beakta relevant **best practice**[40] 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

AMV:s ledningssystem för informationssäkerhet **omfattar** övergripande policydokument som berör ansvarsfördelning och organisation, rutinbeskrivningar för vissa delar av säkerhetsarbetet samt vissa tekniska säkerhetsåtgärder. Dessa **komponenter** är **beslutade** och **dokumenterade**.

Det viktigaste styrdokumentet som rör informationssäkerheten inom AMV är AMV:s *IT-säkerhetspolicy*. IT-säkerhetspolicyn reglerar att en systemsäkerhetsplan ska finnas för varje verksamhetskritiskt IT-system och att varje system ska driftgodkännas utifrån denna. Vidare ska regelbundna penetrationstester genomföras och rutiner för incidenthantering upprättas. Utöver policyn finns regler för Internet och e-post samt riktlinjer för distansarbete. Viktiga *tekniska säkerhetsåtgärder* som finns införda hos AMV är behörighetssystem, virusskydd, brandväggar, säkerhetskopiering av information, flera separerade datorhallar samt Helpdesk.

Det finns dock brister i vissa komponenter, samtidigt som flera komponenter enligt **best practice** saknas.

AMV har inte en samlad dokumenterad överblick över vare sig beslutade eller införda IT-säkerhetsåtgärder (en samlad *åtgärdsplan*, se kapitel 4). Detta

[39] Exempelvis säkerhetschef, systemägare, användare, IT-styrgrupp.

[40] 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.

framgick inledningsvis i granskningen då AMV inte kunde svara på frågan om vissa efterfrågade dokument och komponenter fanns eller inte fanns. Som exempel kan här nämnas kontinuitetsplan och dokumenterade rutiner för säkerhetskopiering av verksamhetskritisk information. Efterfrågade dokument – policyer, riktlinjer, rutinbeskrivningar och annat underlag – visade sig inte heller finnas samlat och direkt tillgängligt inom myndigheten (se bilaga 3).

Granskningen visar att vissa i IT-säkerhetspolicyn beslutade säkerhetsåtgärder inte är fullt **införda**. Systemsäkerhetsplaner finns inte för alla system som uppfattas som verksamhetskritiska. Det finns inte någon fastställd rutin för beslut om driftgodkännande, och sådana beslut fattas därför inte för alla system. Som nämnts i kapitel 4 saknas även dokumenterade rutiner för *incidenthantering*. Penetrationstester har dock genomförts av Försvarets Radioanstalt (FRA).

Policydokumenten för *Internet, e-post och distansarbete* omfattar inte vissa informationssäkerhetsfrågor. Reglerna för Internet och e-post behandlar främst etiska frågor, medan bestämmelser för hur integritetskänsligt eller konfidentiellt material ska sändas, eller krav på att e-postadressen inte ska exponeras på Internet etc. saknas. Riktlinjerna för distansarbete fokuserar på arbetsmiljörelaterade frågor och innefattar inte krav på exempelvis fysiskt skydd, virusskydd och säkerhetskopiering. Virusskydd och säkerhetskopiering ingår dock i IT-plattformen.

AMV:s *IT-säkerhetssamordnare* har ett samordnande ansvar för informationssäkerheten. I rollen ingår ett aktivt uppföljningsansvar för informationssäkerhetsarbetet med rapportering till IT-direktören. Dessutom ingår att stödja systemägare och IT-ansvarig i arbetet med IT-säkerheten för att uppnå IT-säkerhetspolicyns mål. Ledningen har dock inte preciserat under vilka former arbetet med uppföljning och stöd ska ske.

AMV har inte dokumenterade *kontinuitetsplaner* för samtliga verksamheter och verksamhetskritiska IT-system. Det finns inte på ledningsnivå, eller på IT-enheten, någon övergripande kontinuitetsplan med beslut om åtgärder att vidta i händelse av längre avbrott eller längre planerade driftstörningar. Inte heller under intervjuerna har svar kunnat ges på hur sådana händelser ska hanteras. Att längre avbrott har inträffat framgår av kapitel 4. ”Instruktion för AMS/AMV krisledning” har tagits fram av säkerhetschefen, men denna omfattar inte informationssäkerhet. I Riksrevisionens enkät uppger AMV att arbete pågår med en kontinuitetsplan. I granskningen har Riksrevisionen dock inte funnit något formellt beslut eller dokument om detta arbete. I stället har behovet av kontinuitetsplanering inom myndigheten lyfts fram i intervjuerna.

Riksrevisionen konstaterar att AMV inte har någon *åtkomstpolicy*. Tilldelning av behörigheter sker enligt AMV sammanhållet för hela verket för vissa

system, men hanteras delvis separat för andra system. Det finns inte någon dokumenterad rutin för att kontrollera behörigheter. Ett prioriterat arbete påbörjades år 2006 med behörighetsfrågor, exempelvis arbetar IT-stab med att ta fram rollbaserade behörigheter och att centralisera behörighetstilldelningen.

AMV saknar dokumenterade *rutiner för flera viktiga processer*, exempelvis *säkerhetskopiering av verksamhetskritisk information*, patchhantering, och tillägg av nya delar till IT-infrastrukturen. Av intervjuerna framgår att sådant ändå görs och att de tekniska säkerhetsåtgärderna anses vara bra. Det framhålls dock att situationen snarare är ett resultat av enskilda personers intresse av säkerhetsfrågor än av beslutade rutiner. Riksrevisionen konstaterar att personberoendet för vissa säkerhetsåtgärder därmed är högt.

Systemutveckling av interna system inom AMV utförs av IT-enhetens systemsektion. Utvecklingen av ams.se och dess applikationer har hittills utförts av externa leverantörer på uppdrag av systemägaren. Ett utkast till systemutvecklingshandbok finns sedan flera år, men i denna är informationssäkerhetsaspekten endast i viss mån beaktad. Enligt arbetsplanen för IT-enhetens säkerhetsstab (mars 2006) bedrivs inte något organiserat säkerhetsarbete på systemsektionen. Arbete pågår med att ta fram en ny systemutvecklingshandbok, och det finns en medvetenhet inom IT-enheten om att säkerhetsfrågorna måste tas upp tidigt i systemutvecklingsarbetet. De kravbeställningar som ligger till grund för systemutvecklingen görs ofta av systemägarna. Ett problem som IT-enheten lyfter fram är att kraven på säkerheten beaktas för sent eller inte alls i systemutvecklingen. Enligt intervjuer är det inte ovanligt att tilläggsbeställningar av säkerhetsåtgärder kommer sent i utvecklingsarbetet.

Enligt ett beslut på IT-enheten ska systemutvecklingsmodellen inom AMS baseras på RUP, Rational Unified Process, som är ett ramverk för att styra systemutveckling. Enligt AMS pågår ett projekt för införande av RUP, vilket innebär en miljöanpassning till förutsättningar och krav som finns inom AMS. Utkast till projektplan föreligger, men planen är ännu inte fastställd.

IT-enhetens säkerhetsstab anger i sin arbetsplan för år 2006 att de system som AMV själv utvecklar ofta saknar användbar logginformation. AMV har förtydligat detta och anger att i AIS loggas sedan många år både inloggade behöriga användare och felaktiga inloggningsförsök. I och med en lagändring[41] som möjliggjorde att alla handläggare fick tillgång till all information om sökande infördes loggning av exempelvis vilken handläggare som har tittat på vilken sökande. I intervjuer har dock framkommit att syste-

[41] Lag (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.

matisk logghantering eller logginsamling inte görs. Detta försvårar för AMV att i efterhand spåra intrång i systemen. Under år 2006 har IT-enheten påbörjat ett arbete för att förbättra denna situation.

Övriga specifika komponenter som inte finns i jämförelse med LIS-standarden är de verksamhetsansvarigas återkommande *uppföljning av användarnas riskmedvetande och deras kompetens* att hantera informationssäkerhetsriskerna. Vidare finns inte processer för *återkommande uppföljning och förvaltning av komponenterna i ledningssystemet* (se kapitel 7). I Riksrevisionens enkät anger AMV emellertid att myndigheten planerar att införa nämnda komponenter.

I IT-säkerhetspolicyn *beskrivs olika roller* i AMV:s informationssäkerhetsarbete samt det ansvar som följer med dessa. Policyn finns tillgänglig för all personal på AMV:s intranät. Någon samlad information om att en IT-säkerhetspolicy finns har inte lämnats till alla personalgrupper. Riksrevisionen återkommer till detta i kapitel 6.

5.3 Bedömning

Riksrevisionen har funnit brister i införandet och omfattningen av komponenterna i AMV:s ledningssystem för informationssäkerhet, både i jämförelse med vad som bör ingå enligt LIS-standarden och vad AMV:s ledning har beslutat ska finnas. Detta förhållande minskar enligt Riksrevisionens bedömning ledningens möjlighet att förebygga, upptäcka och åtgärda svagheter i myndighetens informationssäkerhet.

Riksrevisionen konstaterar att ledningen inte har skapat tillräckliga möjligheter eller hjälpmedel för att få den överblick som behövs för att ledningen ska kunna övertyga sig om att befintliga och beslutade säkerhetsåtgärder är införda och tillsammans hanterar säkerhetsbrister på ett tillfredställande sätt. På en övergripande nivå saknas en sammanhållen åtgärdslista för säkerhetsåtgärderna och uppföljning av dessa åtgärder. Ledningens bristande möjlighet till överblick och uppföljning kan leda till ett otillräckligt skydd för incidenter och svårigheter att hantera konsekvenserna av dessa.

Sammantaget bedömer Riksrevisionen att konstaterade brister i säkerhetsåtgärderna och uppföljningen av dessa kan påverka AMV:s informationssäkerhet negativt.

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 ledningssystem för informationssäkerhet. 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**[42]. 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 de frågor som kan uppkomma rörande informationssäkerheten.

6.2 Iakttagelser

I det allmänna chefsansvaret, enligt AMS arbetsordning, ingår att initiera informations- och utbildningsinsatser. Enligt IT-säkerhetspolicyn ska varje chef genom utbildnings- eller informationsinsatser ansvara för att medarbetarna har tillräcklig kompetens för att efterleva säkerhetskraven i arbetet. Varje medarbetare är i sin tur skyldig att följa den beslutade IT-säkerhetspolicyn och ta del av och följa de säkerhetsregler som finns för de IT-system som den enskilde användaren har behörighet till. IT-säkerhetspolicyn anger vidare att ledningen, för att förankra IT-säkerhetsarbetet hos samtliga anställda, ska genomföra riktade utbildnings- och informationsinsatser. IT-säkerhetssamordnaren ska biträda vid utbildning i IT-säkerhetsfrågor.

AMV har inte en **process** för systematisk och återkommande information och utbildning beträffande informationssäkerhet till **berörda personalgrupper**, vilket framgår nedan.

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

Under arbetet med IT-säkerhetspolicyn åren 2002 och 2003 skickades den på remiss till bl.a. verksamhetschefer. Cheferna fick därmed inblick i de frågor som policyn kom att omfatta. När beslutet om policyn fattades genomförde IT-staben även en informationsinsats riktad till chefer. Riksrevisionen konstaterar att flertalet chefer under år 2003 bör ha varit insatta i IT-säkerhetspolicyn och dess krav på cheferna att införa och följa upp beslutade IT-säkerhetsåtgärder. Samtliga systemägare och systemförvaltare gick år 2002 ÖCB:s utbildning i FA22 i syfte att lära sig utföra risk- och sårbarhetsanalyser. De som därefter har utsetts till systemägare och systemförvaltare har, enligt vad som framkommit i intervjuer, inte fått motsvarande utbildning.

I samband med att IT-säkerhetspolicyn beslutades av generaldirektören år 2003 fanns långtgående planer på att genomföra policyns krav på informationssäkerhetsutbildning för all personal. Innan information lämnades till de anställda om den nya policyn och det ansvar den medförde ville dock generaldirektören att ett utbildningsprogram skulle tas fram. Generaldirektören gav muntligen i uppdrag åt IT-säkerhetssamordnaren att ta fram ett utbildningsförslag. Möjlighet fanns att vid detta tillfälle utnyttja Försäkringskassans e-utbildning i informationssäkerhet, men AMS utbildningsenhet valde att inte använda denna. I stället skulle enheten ta fram ett eget utbildningsmaterial, vilket inte blev fallet. Enligt en intervju var orsaken att ledningen inte fattade ett formellt beslut i frågan. Följden blev att någon utbildningsinsats inte genomfördes och att det inte gavs någon samlad information till personalen om policyn. Detta har inte heller senare genomförts.

Nyanställda på arbetsförmedlingarna genomgår en introduktionsutbildning. I denna ingår information om Internetregler, men i övrigt behandlas inte ämnet informationssäkerhet. Ansvaret för utbildningen ligger på AMS utbildningsenhet. I takt med ökad nyrekrytering har flera större länsarbetsnämnder genomfört utbildningen själva. AMS har inte bidragit med utbildningsmaterial, vilket skulle ha säkerställt enhetligheten i introduktionsutbildningarna.

Vikten av utbildning inom informationssäkerhetsområdet har under hösten 2005 betonats i verksamhetsplaneringen för ITKT år 2006 och av IT-enhetens säkerhetsstab i arbetsplanen för år 2006. Redan i juni år 2005 påtalades behovet av utbildning av systemförvaltarna av AIS och ams.se i en promemoria[43] som lämnades till enhetschef, IT-ansvarig och IT-säkerhetssamordnare. Några beslut från ledningen med anledning av dessa skrivelser har inte tagits.

[43] IT-säkerhetsarbete 2004 – 2005 på Af-System, PM 2005-06-03.

I Riksrevisionens enkät anger AMV att informationssäkerhetsutbildning inte prioriteras inom myndigheten och därför inte ges till vare sig nyanställda, chefer, myndighetsledning eller övriga medarbetare. Riksrevisionen konstaterar att detta inte är i linje med ledningens krav i IT-säkerhetspolicyn.

I dag kan de anställda informera sig om AMV:s regler för informationssäkerheten på intranätet. Här finns IT-säkerhetspolicyn liksom riktlinjer och regeldokument tillgängliga. Dessa är dock allmänt hållna och riktar sig inte till någon specifik personalkategori.

6.3 Bedömning

Sammantaget bedömer Riksrevisionen att AMV:s ledning inte har säkerställt att personal, systemägare och ansvariga chefer ges tillräcklig och aktuell information om de krav, risker och hot som finns inom informationssäkerhetsområdet. Detta medför enligt Riksrevisionens bedömning en ökad risk för att berörda personalkategorier inte kan fullgöra det ansvar de har. Detta gäller inte minst verksamhetschefernas ansvar att följa upp personalens kunskaper inom informationssäkerhetsområdet och att personalen efterlever de regler som finns.

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 ledningssystem för informationssäkerhet.

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

- Kontrollmiljön: beslutade **delegationer**
- Riskanalys: riskanalysprocess och åtgärdsplanering
- Kontrollfunktioner och säkerhetsåtgärder:
  - genomförande av åtgärdsplanerna,
  - incidentrapporteringen,
  - kontinuitetsplaneringen,
  - den interna kontrollen av utveckling/förändringar i IT-miljö, IT-system och bemanning,
  - den interna kontrollen av tekniska säkerhetsåtgärders funktion (behörighetskontrollsystem, virusskydd, brandväggar m.fl. åtgärder),
  - om den faktiskt uppnådda informationssäkerheten systematiskt prövas och uppfyller säkerhetskraven,
- Information/utbildning: den interna kontrollen beträffande dels information och utbildning angående informationssäkerhet, dels efterlevnaden av det regelverk för upprätthållande av informationssäkerhet som grundas på informationssäkerhetspolicy, Internetpolicy, e-postpolicy, distansarbetspolicy m.fl. policyer.

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

7.2 Iakttagelser

AMV:s ledning har skapat en *kontrollmiljö* där ansvaret för och kontrollen av informationssäkerheten till stor del har delegerats till systemägare, IT-ansvarig, IT-säkerhetssamordnare och IT-direktör. Beslut om rutiner för att ledningen ska kunna kontrollera och följa upp sina **delegationer** finns inte. Av en intervju på ledningsnivå framgår att ledningen förlitar sig på att delegationerna fungerar. Någon uppföljning av att så också är fallet har inte gjorts.

Det finns inget dokument med vägledning för **vidareutveckling** av AMV:s ledningssystem. Det förändringsarbete som sedan år 2006 pågår avseende ledningssystemet sker inte som ett svar på ledningens uppföljning av IT-säkerhetsarbetet. Initiativet kommer i stället främst från personal i organisationen och från utomstående. Detta har lett till att AMV påbörjat ett arbete med att se över sina styrdokument och sitt val av ledningssystem för informationssäkerhetsarbetet.

Det finns inte dokumenterat att ledningen har undersökt om den ansvarsfördelning och organisation som ledningen valt för *risk- och sårbarhetsanalyser* är lämplig samt att den fungerar.

Ledningen har inte en dokumenterad systematisk plan för hur den ska följa upp hur väl viktiga *kontrollfunktioner och säkerhetsåtgärder* fungerar. Enligt intervjuer har den uppföljning som ledningen gjort huvudsakligen begränsats till de tillfällen då allvarliga incidenter har inträffat. Det finns exempel på att uppföljning har gjorts av IT-säkerhetsfrågor. Datainspektionen, FRA samt AMV:s internrevision har genomfört granskningar och tester. Det finns dock ingen dokumentation som visar att ledningen följt upp att åtgärder vidtagits med anledning av rapporterade brister.

Ledningen har inte följt upp att beslutade åtgärder för *information och utbildning* fungerar som avsett. Granskningen visar också att ledningen inte själv har genomfört viktiga utbildnings- och informationsinsatser.

På uppdrag av styrelsen år 2002 genomförde AMV:s ledning ett omfattande arbete under åren 2002 – 2003 med att skapa nödvändiga förutsättningar för arbetet med och organiseringen av informationssäkerheten. Under denna tid tog ledningen viktiga beslut som i dag utgör grunden för AMV:s ledningssystem, även om en översyn för närvarande pågår. En viktig förutsättning var att ledningen valde att bygga sitt ledningssystem på principerna för IT-säkerhet i FA22. Dessa beslut är också utgångspunkt för hur ledningen valde att organisera IT-säkerhetsarbetet och fördela ansvaret i organisationen. Arbetet ledde fram till att den i dag gällande IT-säkerhetspolicyn beslutades. *Rutiner för uppföljning, utvärdering och förvaltning av AMV:s ledningssystem togs dock* inte fram.

Det finns ingen **dokumentation** som visar att ledningen har skapat en rutin för att **systematiskt och regelbundet följa upp** sitt ledningssystem.

Syftet med en sådan rutin är att säkerställa att de förutsättningar som systemet bygger på förblir aktuella och rimliga enligt best practice. Granskningen visar att varken styrelsen eller ledningen följde upp, utvärderade eller diskuterade arbetet med att införa det beslutade ledningssystemet, trots att styrelsen särskilt pekat på behovet av en IT-säkerhetspolicy.

7.3 Bedömning

AMV:s ledning har inte systematiskt följt upp att de förutsättningar och krav som ledningssystemet för informationssäkerhet bygger på är uppfyllda och aktuella. Ett exempel är att delegationerna för informationssäkerhetsarbetet inte har fungerat fullt ut och att ledningen inte har agerat för att få dessa att fungera. Detta innebär enligt Riksrevisionens bedömning att ledningen inte har varit fullt medveten om svagheterna i sitt ledningssystem. Detta försvårar för ledningen att bedöma vilka åtgärder som behöver genomföras för att IT-säkerhetsarbetet ska fungera bättre och i enlighet med beslutad säkerhetsnivå.

Genom att ledningen inte heller har någon utvecklad strategi för hur ledningssystemet ska vidareutvecklas och kvaliteten upprätthållas och förbättras bedömer Riksrevisionen att ledningens möjligheter att förvalta och fatta väl övervägda beslut om utvecklingen av ledningssystemet försämras.

Sammantaget bedömer Riksrevisionen att ledningen inte visat tillräckligt engagemang när det gäller uppföljning av ledningssystemet, vilket innebär en ökad risk för brister i informationssäkerheten inom AMV.

8 Slutsatser och rekommendationer

Ansvaret för styrning och ledning av statsförvaltningens informationssäkerhet är fördelat mellan riksdagen, regeringen, de av regeringen utsedda tillsyns- och stödmyndigheterna samt de enskilda myndigheternas ledningar. Riksrevisionen har i denna granskning valt att fokusera på hur AMV:s myndighetsledning tar sitt ansvar för informationssäkerheten.

Detta kapitel inleds med en sammanfattande bedömning i vilken revisionsfrågan besvaras. Därefter beskrivs de viktigaste bristerna som främst underbygger denna bedömning. Avslutningsvis ges några rekommendationer.

8.1 Slutsatser

Flera komponenter som finns i Riksrevisionens bedömningsgrund, vilken bygger på LIS-standarden (se kapitel 1), finns inte i AMV:s ledningssystem för informationssäkerhet. Detta beror bl.a. på att AMV i april 2003 beslutade att bygga sitt ledningssystem på ÖCB:s FA22[44] som är begränsat i jämförelse med LIS-standarden. En del av de komponenter som AMV har beslutat har införts. Granskningen visar dock på brister i vissa införda komponenter och att andra beslutade komponenter saknas.

Enligt Riksrevisionens bedömning har cheferna inom AMS inte fullt ut genomfört den IT-säkerhetspolicy som beslutades i april 2003, och som är den grundläggande förutsättningen för AMV:s arbete med informationssäkerheten. Detta innebär sammantaget en risk för att organisationens olika delar inte uppfattar och genomför arbetet med informationssäkerhet på ett likartat sätt.

Riksrevisionens samlade bedömning är att AMV:s ledningssystem för informationssäkerhet inte utgör en tillräckligt väl fungerande helhet. En konsekvens av detta är att AMV:s ledning inte kan avgöra om den eftersträvade säkerhetsnivån uppnåtts.

AMV har ingen sammanhållen strategi för att vidareutveckla sitt ledningssystem för informationssäkerhet. Riksrevisionen har dock uppmärksammat att flera insatser är planerade eller pågår för att förbättra ledningssystemet. I april 2006 bestämde IT-direktören att IT-säkerhetspolicyn ska ses över. Av intervjuer framgår också att nuvarande generaldirektör har en ambition att bl.a. få en väl fungerande process för riskanalyser.

[44] FA22 finns inte längre som en produkt som underhålls sedan ÖCB upphörde som myndighet 2002.

Granskningen har haft till syfte att besvara frågan om AMV*, utifrån* gängse normer, arbetar systematiskt med sin informationssäkerhet. Riksrevisionen bedömer sammantaget att *AMV utifrån gängse normer inte fullt ut arbetar systematiskt med sitt ledningssystem för informationssäkerhet.* Bedömningen baseras på tre huvudsakliga brister. Bristerna har redan beskrivits mer ingående i de tidigare kapitlen. Nedan sammanfattas beskrivningen av brister.

8.1.1 Ledningen har inte tillräckligt väl styrt och kontrollerat informationssäkerhetsarbetet

På initiativ av dåvarande styrelsen genomförde ledningen ett grundläggande arbete åren 2002–2003 för att få fram en väl förankrad IT-säkerhetspolicy. Granskningen visar att ledningen inte i tillräcklig utsträckning har genomfört och följt upp beslutade åtgärder i IT-säkerhetspolicyn. Ett flertal säkerhetsåtgärder har inte införts. Som exempel kan nämnas att nödvändiga riktlinjer och instruktioner för IT-säkerhetsarbetet inte tagits fram, att arbetet med riskanalyser inte är samordnat och att utbildningsinsatser inte har genomförts. Det finns ingen systematisk utbildningsprocess för att säkerställa att nyckelpersoner inom säkerhetsarbetet får tillräcklig och återkommande utbildning inom området. Det finns vidare oklarheter om fördelningen av ansvaret för säkerhetsarbetet, vilket bl.a. lett till att kommunikation och samverkan mellan olika aktörer i informationssäkerhetsarbetet försvårats. En konsekvens av detta är att säkerhetsarbetet inte har hanterats sammanhållet och att ledningen inte fått kontinuerlig information om de brister som finns i IT-säkerheten. Ledningen har därmed inte utifrån ett helhetsperspektiv agerat för att uppfylla IT-säkerhetspolicyns mål och uppnå den säkerhetsnivå som beslutats.

Riksrevisionens slutsats är att ledningen inte tillräckligt väl har styrt och kontrollerat informationssäkerhetsarbetet. Om ledningens beslut i IT-säkerhetspolicyn hade införts fullt ut skulle AMV i dag ha betydligt bättre förutsättningar för att med kompletterande åtgärder nå upp till LIS-standarden som utgör best practice inom informationssäkerhetsområdet.

8.1.2 Riskanalysen är ofullständig

Arbetet med riskanalyser inom AMV bedrivs inte i linje med ledningens beslut i IT-säkerhetspolicyn. Arbetet är inte tillräckligt organiserat, informationstillgångarna säkerhetsklassas inte, riskanalyser har inte genomförts och systemsäkerhetsplaner har inte tagits fram för alla IT-system. Det finns inte heller gemensamma modeller och metoder för ett sådant arbete. Vissa utvecklingsinsatser i denna riktning har dock genomförts. Inträffade

incidenter pekar på att faktiska svagheter i riskanalyserna och otillräckliga säkerhetsåtgärder förekommit.

Någon samlad riskbedömning och åtgärdsplan för AMV:s informationssäkerhet finns inte. Ledningen har inte heller efterfrågat detta. Enligt Riksrevisionens bedömning begränsas därmed ledningens möjlighet att överblicka och följa upp riskerna för myndighetens verksamhet samt upprätta en samlad åtgärdsplan för investeringar som görs i informationssäkerhet.

8.1.3 Uppföljning och vidareutveckling av ledningssystemet för informationssäkerhet är otillräcklig

Grunden för det ledningssystem som AMV:s ledning har valt är FA22, vilket bl.a. innebär en långtgående decentralisering och delegering av informationssäkerhetsarbetet. Fokus läggs på systemägare och deras ansvar för säkerheten i enskilda system. Ledningen har inte systematiskt följt upp och dokumenterat att de förutsättningar och krav som AMV:s ledningssystem bygger på är uppfyllda och aktuella. Riskerna med det valda ledningssystemet har inte analyserats. Därmed har ledningen enligt Riksrevisionens bedömning inte kunnat konstatera i vilken utsträckning ledningssystemet fungerar som avsett och inte heller kunnat bedöma behovet av att vidareutveckla ledningssystemet. En strategi för vidareutveckling av ledningssystemet saknas. Detta har lett till att ledningen inte uppmärksammat brister i sitt ledningssystem.

8.2 Rekommendationer

Riksrevisionens bedömning är att ett sammanhållet och tydligt ledningssystem för informationssäkerhet är en förutsättning för att AMV:s ledning ska kunna förvissa sig om att beslutade säkerhetsnivåer införs och bibehålls i hela myndigheten. Detta kräver bl.a. att ledningssystemet omfattar hela AMV och är integrerat med övriga ledningssystem. Det bör ge ledningen möjlighet till överblick över risker och skillnader i risker mellan olika verksamheter, behovet av säkerhetsåtgärder och kostnader för säkerhetsarbetet i de olika verksamheterna. Då framstår också tydligare vilket utrymme som finns för prioriteringar mellan säkerhetsinvesteringar i skilda delar av myndigheten. Den i granskningen använda LIS-standarden innehåller enligt Riksrevisionens bedömning de viktigaste kraven på ett sådant ledningssystem.

AMV:s ledning bör vidare ställa krav på sitt ledningssystem som beaktar de allvarliga konsekvenser som kan inträffa om IT-systemen inte är säkra. Felaktiga uppgifter i AMV:s register till följd av bristande informationssäkerhet kan få omfattande konsekvenser.

Några exempel på tänkbara konsekvenser av brister i informationssäkerheten är:

- att sekretessbelagda personuppgifter röjs,
- att enskild person lider ekonomisk skada då underlag till a-kassa är fel och beslut fattas på felaktiga grunder,
- att statistikunderlag och uppföljningar till bl.a. regering och riksdag blir missvisande,
- att matchning av arbetssökande med arbetsgivarnas lediga platser inte får full effekt på grund av bristfällig registerkvalitet.

AMV har under år 2006 påbörjat ett viktigt arbete med att förbättra sitt ledningssystem för informationssäkerhet. Riksrevisionen rekommenderar AMV beakta följande i detta arbete.

- Ledningen bör utforma sitt ledningssystem för informationssäkerhet så att den kan förvissa sig om att beslutade säkerhetsnivåer införs och bibehålls i hela myndigheten. I detta bör ingå att precisera och fastställa hur säkerhetsarbetet ska bedrivas och då tydliggöra ansvarsfördelning, samordning, utbildningsinsatser och rapporteringsvägar inom organisationen.
- I AMV:s ledningssystem bör ingå en systematisk process för myndighetens riskanalysarbete. En sådan process skulle ge ledningen möjlighet att överblicka risker för hela AMV, skillnader i risker mellan olika verksamheter, behov av säkerhetsåtgärder och kostnader för säkerhetsarbetet i de olika verksamheterna. Då framträder tydligare vilket utrymme som finns för prioriteringarna mellan säkerhetsinvesteringar i skilda delar av myndigheten. Dessa prioriteringar bör samlas i en åtgärdsplan. Ledningen bör med denna plan följa upp att beslutade åtgärder införs och fungerar som avsett. Den bör vidare utformas så att de resurser som ägnas säkerhetsarbetet kan beskrivas, följas och utvärderas.
- Ledningen bör systematiskt följa upp hur ledningssystemet fungerar, och om de förutsättningar och krav som ledningssystemet bygger på är uppfyllda och aktuella. Detta bör ske som en del av en strategi för vidareutveckling av ledningssystemet.

Bilaga 1 Huvudsakliga skillnader mellan FA22 och BITS

I denna bilaga beskrivs översiktligt skillnaden mellan FA22, som AMV valt som grund för sitt IT-säkerhetsarbete, och BITS som AMV numera strävar efter att uppnå.

Förenklat innebär säkerhetsprocessen enligt FA22:

- Myndigheten ska definiera målen och inriktningen för sitt säkerhetsarbete i en säkerhetspolicy.
- Utifrån säkerhetspolicyn tas en systemsäkerhetsplan fram för varje enskilt samhällsviktigt datasystem. I systemsäkerhetsplanen identifieras utöver grundsäkerheten s.k. tilläggskrav. Detta är en sammanfattande beteckning på övriga styrande lagkrav, verksamhetskrav på sekretess, tillförlitlighet och tillgänglighet samt hotbild.
- Utifrån säkerhetspolicyn och systemsäkerhetsplanen tas också säkerhetsinstruktioner fram där det fastställs vilka säkerhetsregler som gäller.
- De i systemsäkerhetsplanen fastställda kraven innebär att vissa säkerhetsåtgärder kan behöva vidtas. Föreskrifterna i FA22 redovisar åtgärder för att tillgodose grundsäkerheten. Övriga åtgärder som behövs enligt systemsäkerhetsplanen måste fastställas av systemägaren.
- För att kontrollera att vidtagna säkerhetsåtgärder i datasystemet uppfyller ställda krav genomförs en granskning av befintliga säkerhetsåtgärder i datasystemet. Granskningen leder till att en säkerhetsutvärdering kan genomföras. Denna säkerhetsutvärdering ligger till grund för beslut om driftgodkännande av datasystemet.

De olika stegen i säkerhetsprocessen är i BITS relativt lika FA22. En viktig skillnad jämfört med FA22 är dock att BITS omfattar hela begreppet informationssäkerhet medan FA22 betonar datasystemsäkerhet. FA22 betonar också samhällsviktiga datasysystem medan BITS talar om informationssystem som bedöms viktiga för verksamheten.

BITS understryker genomförandet av risk- och sårbarhetsanalyser, att det ska finnas en struktur för riskbedömning och riskhantering samt ledningens engagemang i beslut om godtagbar risknivå och övriga informationssäkerhetsfrågor. FA22 framhäver i högre grad systemägarens ansvar för IT-säkerheten. Det ska enligt BITS finnas en av ledningen fastställd informationssäkerhetspolicy som ska uttrycka bl.a. ledningens engagemang samt en struktur för riskbedömning och riskhantering. Även om informationssäkerhetsarbetet oftast utförs av säkerhetsorganisationen måste ledningen vara nära involverad eftersom arbetet ska spegla ledningens viljeinriktning.

Ledningen ska också besluta om vilken risknivå som kan godtas. Utgångspunkten för arbetet med informationssäkerhet är enligt BITS att risk- och sårbarhetsanalyser genomförs för att klargöra vilken säkerhetsnivå som ska gälla. Basnivån enligt BITS är endast en lägsta nivå som inte får underskridas.

I BITS har också, till skillnad från i FA22, begreppet informationssäkerhetssamordnare/-funktion en central betydelse. En person eller en grupp av personer ska utgöra den sammanhållande länken mellan den operativa verksamheten för informationssäkerhet och ledningen.

Bilaga 2 Uppgifter om vissa informationssystem inom Arbetsmarknadsverket

I rapporten avsnitt 2.2 ges mer översiktliga uppgifter om AMV:s IT-system. I denna bilaga ges ytterligare information om delsystem och särskilda tjänster för vissa IT-system.

Arbetsmarknadsverkets InformationsSystem – AIS

AIS är den offentliga arbetsförmedlingens interna informationssystem, och informationen i systemet utgör AMV:s myndighetsregister.

Delsystem inom AIS är följande:

Order: Här registrerar arbetsförmedlingen manuellt 30 procent av de lediga platserna. Merparten registreras av arbetsgivarna i AIS via www.ams.se (se nedan).

Arbetsgivare: Här registrerar arbetsförmedlingen uppgifter om företag, organisationer och privatpersoner som förmedlingen varit i kontakt med. Arbetsgivare kan registrera sig själva via www.ams.se (se nedan) och blir då Internetarbetsgivare i AIS.

Handläggare: Här finns uppgifter registrerade om alla handläggare inom AMV med behörighet i AIS.

Kontor: Här finns uppgifter registrerade om alla förmedlingskontor inom AMV.

Sökande: Här finns alla arbetssökande registrerade med bl.a. uppgifter om a-kassa, handlingsplan, daganteckningar samt grunduppgifter för matchning.

Yrkesmall: Nyckelbegrepp för ett yrke samt underlag och hjälpmedel för att beskriva sökandes kompetens och arbetsgivares krav på kompetens för ledig plats i AIS.

Ärende (program/insats): Här registrerar arbetsförmedlaren anvisningar och tar beslut om program och insatser.

Projekt: Här administrerar arbetsförmedlaren medel för projekt och projekt med arbetsmarknadspolitisk inriktning.

Arbetsmarknadsverkets webbplats www.ams.se

AMV:s webbplats är en informationskanal för målgrupperna arbetssökande, arbetsgivare samt informationssökande. Webbplatsen delas in i sex huvudområden:

Söka jobb: Ger stöd för målgruppen arbetssökande i form av självserviceverktyg och information.

Rekrytera: Ger stöd för målgruppen arbetsgivare i form av självserviceverktyg och information.

Yrken/studier: Ger stöd för målgruppen arbetssökande/ informationssökande i form av självserviceverktyg och information.

Arbetsförmedlingar: Ger stöd för samtliga målgrupper, information om Arbetsförmedlingens servicekanaler, tjänsteutbud, självserviceverktyg för e-tjänster och inskrivning vid arbetsförmedling.

Nyheter/fakta: Ger stöd för samtliga målgrupper med information om exempelvis arbetsmarknad, prognoser, och pressmeddelanden.

Om AMV: Ger stöd för samtliga målgrupper, information om AMV:s organisation, struktur och ledning.

Självserviceverktyg på www.ams.se – Af Internet (AFI)

På AMV:s webbplats www.ams.se finns de självserviceverktyg (AFI) som används av målgrupperna arbetssökande, arbetsgivare och arbetsförmedlare. Både externa och interna parter utför aktiviteter inom den verksamhet AFI stöder. Externa parter utgörs av arbetssökande, arbetsgivare, övriga informationslämnare och informationshämtare, exempelvis press och medborgare. Interna parter utgörs av arbetsförmedlare, redaktörer, informationsproducenter samt informatörer.

AFI består av ett trettiotal publika applikationer i fyra publika portaler samt elva icke publika applikationer i en handläggarportal. Dessa applikationer fördelas på ams.se mellan huvudområdena *Söka jobb, Rekrytera, Yrken/studier samt Arbetsförmedlingar*. Ur användarsynpunkt är webbplatsen dock en och samma portal.

Det finns ett antal verksamhetsstöd skapade utifrån målgrupperna i verksamheten för att skapa preciserade leveranser från förvaltningsverksamheten:

- e-kanal: Ger möjlighet till presentation av information och tjänsteutbud, kommunikation mellan aktörer samt lagring av personliga/organisatoriska data i AMV:s databaser.
- e-matchning: Ger arbetssökande, arbetsgivare och arbetsförmedlare stöd i matchning via e-kanalen.
- e-myndighetsutövning: Möjliggör för arbetsförmedlare att delar av AMV:s myndighetsutövning kan ske via e-kanalen.

- publiceringsstöd: Möjliggör för redaktörer och informatörer att informera via e-kanalen.
- e-kunskapsstöd: består av information som vänder sig till både samtliga intressenter och till förvaltningsorganisationen.

Bilaga 3 Dokument från Arbetsmarknadsverket

Under granskningens gång har Riksrevisionen fått ta del av och granskat dokument (allmänna handlingar inom AMV) som beskriver olika delar av AMV:s ledningssystem för informationssäkerhet. Riksrevisionen har granskat dessa dokument utifrån bedömningsgrunden (LIS-standarden i kombination med COSO, se kapitel 1).

Ledningens kontrollmiljö

Dokument som visar vilka förutsättningar som ledningen skapat för arbetet med informationssäkerheten. Det avser bl.a. organisatoriska former för arbetet, stöd till de som arbetar med informationssäkerhet samt resurser.

AMV/AMS Krisledning. 2006-02-09.

Arbetsordning för Arbetsmarknadsstyrelsen.

Arbetsordning för Arbetsmarknadsverket. 2003-04-25.

Arbetsmarknadsverkets organisation i maj 2006.

Befattningsbeskrivning IT-säkerhetssamordnare. Utkast 2003-03-10 ej beslutad.

Beslut om ny AMS Säkerhetsskyddschef. 2006-02-01.

Dokument om krisberedskapsarbete/krishantering upprättat av säkerhetschefen. 2005-12-22.

Ekonomisystem och förvaltare (förteckning).

En kompetent IT-resurs. 2004-10.

Förordning (2001:623) med instruktion för Arbetsmarknadsverket. 2001-07-05.

Förvaltningsobjekt inom AMV. 2006-04-11.

Instruktion för AMS/AMV krisledning. 2006-02-09.

IT-enheten (organisationsskiss). 2006-01-01.

IT-säkerhetspolicy för Arbetsmarknadsverket. 2003-04-30.

Krishantering, AMS Förvaltningsavdelningen. 2005-12-22.

Krisledningsgruppen för Af Internet. 2005-11-07.

Modell för systemförvaltning inom AMV v 1.1. maj 2004.

Modell för systemförvaltning inom AMV v 2.0. maj 2006 utkast.

Organisation av säkerhetsarbetet inom AMS. 2005-07-07.

Regleringsbrev för budgetåret 2006 avseende Arbetsmarknadsverket (AMV) och anslag inom utgiftsområde 13 Arbetsmarknad. Näringsdepartementet, 2005-12-20.

Styrelseprotokoll AMS styrelse 2005-02-18.

Säkerhetsstaben Arbetsplan 2006. 2006-03-06.

Säkerhetsskyddsplan för AMS. 2005-07-06.

Ändring av regleringsbrev för budgetåret 2005 avseende Arbetsmarknadsverket (AMV) och anslag inom UO13 Arbetsmarknad. Näringsdepartementet, 2005-06-22.

Riskanalys och prioritering av säkerhetsåtgärder

Dokument som visar hur arbetet med risk- och sårbarhetsanalyser organiseras och styrs. I arbetet bör ingå förteckning över informationstillgångar, informations- och säkerhetsklassning, metoder, riskidentifiering, incidentrapportering och -analys, och åtgärdsplan.

AMS budget 2005 – Tillägg från Avdelningen för informations- och kommunikationsteknik. 2004-12-07.

Analys av säkerhetskraven på de verksamhetskritiska delarna av ams.se samt att översiktligt beskriva åtgärder för att uppfylla dessa krav. Maj 2004.

Budget 2005 –Avdelningen för informations- och kommunikationsteknik . Förslag 2005-02-01.

Etableringen av AMS Förvaltningsmodell på Förvaltningsobjektet – AIS, En förvaltningsanalys och utvärdering. Yarrow Consulting AB, 2006-04-01.

Förvaltningsanalys AIS version 1.6.

Förvaltningsanalys AIS (PowerPoint-presentation*)*. Yarrow Consulting AB.

Förvaltningsobjekt inom AMV.

*IT-säkerhetsarbete 2004 – 2005 på AF-system.*2006-06-03.

Kopia av rapport från Helpdesk.

Områdesriskbedömning (AMS SSO-projektet). 2002-04-17.

Projektportföljer per organisatorisk enhet. 2006.

Riskidentifiering och riskanalys (Excel-mall). Länsarbetsnämnden i Stockholms län.

Risk- och sårbarhetsanalys av AMV:s IT-miljö. 2001-02-06.

Risk- och sårbarhetsanalys 2005, årlig rapportering. 2006-02-17.

Systemförteckning. 2006-04-11.

Systemsäkerhetsplan Åtgärdssystemet. 2002-03-07.

Säkerhetsplan för www.ams.se. 2005-03-21.

Systemsäkerhetsplan AIS 2006. 2005-12-08.

Säkerhetsåtgärder för ams.se Basnivå för IT-säkerhet (BITS). maj 2004.

Säkerhetsåtgärder för ams.se Komplettering från LIS. Maj 2004.

Verksamhetsplan 2006. 2006-01-03.

Verksamhetsplan år 2005 för Arbetsmarknadsverket. 2005-01-05.

Verksamhetsplan 2006-2008 – IKT-avdelningen. 2005-11-23.

Verksamhetsplan 2006 – Avdelningen för IT och kundtjänst. 2006-01-25.

Kontrollfunktioner och säkerhetsåtgärder

Dokument som visar vilka beslutade och dokumenterade säkerhetsåtgärder som ledningen utformat för att förebygga, upptäcka och åtgärda brister i informationssäkerheten. Med åtgärder avses bl.a. styrdokument, regler och rutinbeskrivningar, tekniska skyddsåtgärder samt åtgärder för att följa upp skyddet.

Af Internet Reservrutiner för arbetsförmedlingar, arbetssökande och arbetsgivare. 2005-11-07.

Af Internet Reservrutiner för Externa informationshämtare. 2005-11-07.

Arbetsmarknadsstyrelsens administrativa föreskrifter (AMSFS 2002:12) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten. 2002-10-18.

Arbetsmarknadsstyrelsens föreskrifter (AMSFS 2002:11) om tillämpningen av lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten. 2002-10-18.

Behörighet i AMV:s system. 2003-10-10.

Behörighetsbeskrivning för förmedlingssystemet AIS. 2004-10-08.

Design Programmeringsstandard för Java webbapplikationer. 2006-05-03.

Driftgodkännande AIS. 2005-12-08.

Förordning (2002:623) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten. Regeringen, 2002-06-13.

Förvaltningsplan för AIS 2006. 2005-09-08.

Förvaltningsplan AIS 2006 Bilagor. 2004-11-30.

Förvaltningsplan AFI. 2006-04-01.

Förvaltningsplan AFI 2006 Bilagor. april 2006.

Lag (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.

Interna regler för e-posten och Internet. 2003-12-13.

Prioritet för supportuppdrag. IT-enheten, 2004-08-17.

Projektdirektiv RUP, AMS 2004-11-09.

Protokoll över inspektion enligt personuppgiftslagen (1998:204) och lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten. Datainspektionen, 2004-06-14.

Riktlinjer för distansarbete gällande hela AMV. 2003-06-23.

Sammanställning av förutsättningar för kontinuitetsplan för Af Internet. 2005-05-26.

Systemutvecklingshandbok version 1.1.

Säkerhetsprövning av person innan anställning inom AMS, 2006-03-03.

Säkerhetsplan för ams.se. 2005-03-21.

Information och utbildning

Dokument som visar ledningens åtgärder för att förse personalen med information och kunskaper om informationssäkerhet. Vidare ingår åtgärder som ger ledningen information om personalens kunskapsnivå, bl.a. genom chefernas uppföljning av att personalen följer gällande regler. Information och utbildning bör ges inom en process för systematisk och återkommande information och utbildning.

Arbetsmarknadsverket satsar på IT-säkerhet. 2003-11-12 dnr VLK 02-001866-06.

Informationssäkerhet (från VIS). 2003-07-29.

Introduktionsutbildning vid länsarbetsnämnd.

PM för beställning av offert för e-utbildning i IT-säkerhet. IT-stab, 2003-04-24 dnr VLK 02-001866-06.

Systemsäkerhet (från VIS). 2006-01-31.

Uppföljning och förvaltning

Dokument som visar hur ledningen följer upp den interna styrningens och kontrollens utformning och effektivitet. Uppföljningen ska vara systematisk, regelbunden och dokumenterad.

AMS kompletterande synpunkter på Datainspektionens protokoll, 939-2004. 2004-08-30.

Ang Revisionsuppdrag "Behörighetsadministration och behörighetskontrollsystem för handläggarsystemet AIS". 2006-02-20.

Arbetsmarknadsstyrelsens (AMS) svar på enkätfrågor om informationssäkerhet. 2004-08-24.

Arbetsmarknadsstyrelsens (AMS) svar på "Frågeställningar med anledning av inspektioner vid länsarbetsnämnder Arbetsmarknadsstyrelsen" från Datainspektionen med dnr 939-2004, daterad 2004-11-12. 2004-11-29.

Arbetsmarknadsverkets revisionsplaner 2001–2006. AMS Internrevision. Omfattar bl.a. riskanalyser av AMV:s IT-verksamhet.

Bilaga IT-säkerhet. Datainspektionen.

Granskning av behörighetsadministration och behörighetskontrollsystem för handläggarsystemet AIS. AMS Internrevision, 2006-01-12.

Granskning av Grundsäkerhet i samhällsviktiga IT-system. AMS Internrevision, 2003-01-14.

Granskning av löner och andra ersättningar samt datasystemet Palasso. AMS Internrevision, 2003-09-10.

Handlingsplan (AMS SSO-projektet). 2002-12-04.

Presentation för IT-ledningsgruppen 13 mars 2002 av "AMS Projektrevision av SSO-projektet". Cap Gemini Ernst & Young.

Programenhetens svar på Granskning av Grundsäkerhet i samhällsviktiga IT-system. 2003-02-05.

Projektrevision av SSO-projektet (version 1.1). Cap Gemini Ernst & Young, 2002-03-13.

Sammanfattning av SSO-audit. PM 2003-05-14.

Svar på Granskning av Grundsäkerhet i samhällsviktiga IT-system. AMS, 2003-02-17.

Uppföljning av granskning av löne- och PA-systemet Palasso. AMS Internrevision, 2005-11-11.

Viktiga slutsatser från CAP:s audit. 2002-04-16.

Överenskommelse om säkerhetsgranskning. FRA, 2003-09-08.

Övrigt

Dokument som visar AMV:s uppfattning om informationssäkerhet.

Remissvar avseende Slutbetänkande Informationssäkerhetspolitik – organisatoriska konsekvenser (SOU 2005:71) dnr Fö2005/2204/CIV, AMS, Remissvar på "Slutbetänkande Informationssäkerhetspolitik – Organisatoriska konsekvenser (SOU 2005:71)". 2006-01-03.

Remiss Statskontoret Dnr 2004/203-5 "Förslag betr. Föreskrifter om informationssäkerhet för 24-timmarsmyndigheter". 2005-03-23.

Svar på Riksrevisionens frågeformulär avseende myndigheternas arbete med informationssäkerhet. 2006-04.

Källförteckning

Lagar

Arkivlag (1990:782)

Lag (2003:389) om elektronisk kommunikation

Lagen (1990:217) om skydd för samhällsviktiga anläggningar m.m.

Personuppgiftslag (1998:204)

Sekretesslag (1980:100)

Säkerhetsskyddslag (1996:627)

Tryckfrihetsförordning (1949:105)

Förordningar

Arkivförordning (1991:446)

Förordningen (SFS 2001:623) med instruktion för Arbetsmarknadsverket

Förordning (2006:942) om krisberedskap och höjd beredskap

Förordning (1995:1300) om myndigheters riskhantering

Personuppgiftsförordning (1998:1191)

Säkerhetsskyddsförordning (1996:633, 2000:888)

Verksförordning (1995:1322)

Föreskrifter och allmänna råd

Datainspektionen 1999. *Säkerhet för personuppgifter*

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

Krisberedskapsmyndigheten 2006. *Basnivå för informationssäkerhet KBM rekommenderar 2006:1.*

Rikspolisstyrelsen 1996. *Föreskrifter om säkerhetsskydd (RPS FS 1996:9 FAP 244-1)*

Överstyrelsen för civil beredskap 1998. *Föreskrifter om grundsäkerhet för samhällsviktiga datasystem hos beredskapsmyndigheter (ÖCB fs 1998:1)*. I syfte att förtydliga föreskrifterna meddelade ÖCB allmänna råd till dessa. Föreskrifterna och de allmänna råden kallas FA22 (Föreskrifter och Allmänna råd till då gällande beredskapsförordning (1993:242) 22 a § och 52 §).

Standarder

SS-ISO/IEC 17799, SS 627799. *Ledningssystem för informations-säkerhet.*

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

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.*

Texter från Internet

ISACA. *Control Objectives for Information and related Technology (COBIT).* http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

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*

Nationella revisionsorgan

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

Tidigare utgivna rapporter från Riksrevisionen

2003	2003:1	Hur effektiv är djurskyddstillsynen?
2004	2004:1	Länsplanerna för regional infrastruktur – *vad har styrt prioriteringarna?*
	2004:2	Förändringar inom kommittéväsendet
	2004:3	Arbetslöshetsförsäkringens hantering på arbetsförmedlingen
	2004:4	Den statliga garantimodellen
	2004:5	Återfall i brott eller anpassning i samhället *– uppföljning av kriminalvårdens klienter*
	2004:6	Materiel för miljarder – *en granskning av försvarets materielförsörjning*
	2004:7	Personlig assistans till funktionshindrade
	2004:8	Uppdrag statistik *Insyn i SCB:s avgiftsbelagda verksamhet*
	2004:9	Riktlinjer för prioriteringar inom hälso- och sjukvård
	2004:10	Bistånd via ambassader *– en granskning av UD och Sida i utvecklingssamarbetet*
	2004:11	Betyg med lika värde? – *en granskning av statens insatser*
	2004:12	Höga tjänstemäns representation och förmåner
	2004:13	Riksrevisionens årliga rapport 2004
	2004:14	Arbetsmiljöverkets tillsyn
	2004:15	Offentlig förvaltning i privat regi *– statsbidrag till idrottsrörelsen och folkbildningen*
	2004:16	Premiepensionens första år
	2004:17	Rätt avgifter? – *statens uttag av tvingande avgifter*
	2004:18	Vattenfall AB – *Uppdrag och statens styrning*
	2004:19	Vem styr den elektroniska förvaltningen?
	2004:20	The Swedish National Audit Office Report 2004
	2004:21	Försäkringskassans köp av tjänster för rehabilitering
	2004:22	Arlandabanan *Insyn i ett samfinansierat järnvägsprojekt*
	2004:23	Regelförenklingar för företag
	2004:24	Snabbare asylprövning
	2004:25	Sjukpenninganslaget – utgiftsutveckling under kontroll?
	2004:26	Utgift eller inkomstavdrag? – Regeringens hantering av det tillfälliga sysselsättningsstödet
	2004: 27	Stödet till polisens brottsutredningar
	2004:28	Regeringens förvaltning och styrning av sex statliga bolag
	2004:29	Kontrollen av strukturfonderna
	2004:30	Barnkonventionen i praktiken
2005	2005:1	Miljömålsrapporteringen – *för mycket och för lite*
	2005:2	Tillväxt genom samverkan?

2005:3 Arbetslöshetsförsäkringen – *kontroll och effektivitet*
2005:4 Miljögifter från avfallsförbränningen – *hur fungerar tillsynen*
2005:5 Från invandrarpolitik till invandrarpolitik
2005:6 Regionala stöd – *styrs de mot ökad tillväxt?*
2005:7 Ökad tillgänglighet i sjukvården? – *regeringens styrning och uppföljning*
2005:8 Representation och förmåner i statliga bolag och stiftelser
2005:9 Statens bidrag för att anställa mer personal i skolor och fritidshem
2005:10 Samordnade inköp
2005:11 Bolagiseringen av Statens järnvägar
2005:12 Uppsikt och tillsyn i samhällsplaneringen – *intention och praktik*
2005:13 Riksrevisionens årliga rapport 2005
2005:14 Förtidspension utan återvändo
2005:15 Marklösen *Finns förutsättningar för rätt ersättning?*
2005:16 Statsbidrag till ungdomsorganisationer – *hur kontrolleras de?*
2005:17 Aktivitetsgarantin – *Regeringen och AMS uppföljning och utvärdering*
2005:18 Rikspolisstyrelsens styrning av polismyndigheterna
2005:19 Rätt utbildning för undervisningen *Statens insatser för lärarkompetens*
2005:20 Statliga myndigheters bemyndiganderedovisning
2005:21 Lärares arbetstider vid universitet och högskolor – *planering och uppföljning*
2005:22 Kontrollfunktioner – *två fallstudier*
2005:23 Skydd mot mutor *Läkemedelsförmånsnämnden*
2005:24 Skydd mot mutor *Apoteket AB*
2005: 25 Rekryteringsbidrag till vuxenstuderande – *uppföljning och utbetalningskontroll*
2005:26 Granskning av Statens pensionsverks interna styrning och kontroll av informationssäkerheten
2005:27 Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten
2005:28 Fokus på hållbar tillväxt? *Statens stöd till regional projektverksamhet*
2005:29 Statliga bolags årsredovisningar
2005:30 Skydd mot mutor *Banverket*
2005:31 När oljan når land – *har staten säkerställt en god kommunal beredskap för oljekatastrofer?*

2006 2006:1 Arbetsmarknadsverkets insatser för att minska deltidsarbetslösheten
2006:2 Regeringens styrning av Naturvårdsverket
2006:3 Kvalitén i elöverföringen – *finns förutsättningar för en effektiv tillsyn*
2006:4 Mer kemikalier och bristande kontroll – *tillsynen av tillverkare och importörer av kemiska produkter*

2006:5 Länsstyrelsernas tillsyn av överförmyndare
2006:6 Redovisning av myndigheters betalningsflöden
2006:7 Begravningsverksamheten – *förenlig med religionsfrihet och demokratisk styrning?*
2006:8 Skydd mot korruption i statlig verksamhet
2006:9 Tandvårdsstöd för äldre
2006:10 Punktskattekontroll – mest reklam?
2006:11 Vad och vem styr de statliga bolagen?
2006:12 Konsumentskyddet inom det finansiella området – fungerar tillsynen?
2006:13 Kvalificerad yrkesutbildning – *utbildning för marknadens behov?*
2006:14 Arbetsförmedlingen och de kommunala ungdomsprogrammen
2006:15 Statliga bolag och offentlig upphandling
2006:16 Socialstyrelsen och de nationella kvalitetsregisten inom hälso- och sjukvården
2006:17 Förvaltningsutgifter på sakanslag
2006:18 Riksrevisionens Årliga rapport
2006:19 Statliga insatser för nyanlända invandrare
2006:20 Styrning och kontroll av regeltillämpningen inom socialförsäkringen
2006:21 Finansförvaltningen i statliga fastighetsbolag
2006:22 Den offentliga arbetsförmedlingen
2006:23 Det makroekonomiska underlaget i budgetpropositionerna

Beställning: publikationsservice@riksrevisionen.se