RIKSREVISIONEN

Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten

ISBN 91 7086 093 9
RiR 2006:25
Tryck: Riksdagstryckeriet, Stockholm 2006

Till regeringen
Utrikesdepartementet

Datum 2006-11-29
Dnr 31-2006-0307

Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten

Riksrevisionen har granskat den interna styrningen och kontrollen av informationssäkerheten vid Migrationsverket. Granskningen ingår i en serie av granskningar som genomförs vid statliga myndigheter avseende informationssäkerhet. Resultatet av granskningen redovisas i denna rapport. Företrädare för Migrationsverket har beretts tillfälle att faktagranska och lämna synpunkter på utkast till denna granskningsrapport.

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

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

Riksrevisor *Karin Lindell* har beslutat i detta ärende. Granskningen har genomförts av revisionsledare *Annika C Karlsson* (föredragande), revisionsledare *Frank Lantz* och revisor *Peter Mårtensson*. Biträdande granskningsområdeschef *Rutger Banefelt* och revisionsdirektör *Björn Undall* har medverkat i den slutliga handläggningen.

Karin Lindell

Annika C Karlsson

För kännedom:
Migrationsverket

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 verksledningen tar sitt ansvar för informationssäkerheten.

Under 2005-2006 har Riksrevisionen granskat informationssäkerheten vid tio statliga myndigheter. Denna granskning fokuserar på hur Migrationsverket 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 så kallade LIS-standarden (SS-ISO/IEC 17799). LIS-standarden beskriver hur ett välfungerande 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?

Migrationsverket har en omfattande hantering av personuppgifter. Brister i Migrationsverkets förmåga att skydda sina informations-

tillgångar kan leda till skada för enskilda personer. Om inte personuppgifter hanteras korrekt kan detta leda till fel i handläggningen av asyl-, tillstånds- och medborgarskapsärenden vilket i slutändan kan leda till att fel beslut fattas. Ett positivt beslut om asyl samt beslut om medborgarskap kan inte återkallas oavsett om beslutet har fattats på fel grunder. Brister i förmågan att skydda informationstillgångarna kan också äventyra allmänhetens förtroende för Migrationsverket.

Har Migrationsverket ett väl fungerande ledningssystem för informationssäkerhet?

Ett sammanhållet och tydligt ledningssystem för informationssäkerhet är en förutsättning för att Migrationsverkets ledning ska kunna förvissa sig om att beslutade säkerhetsnivåer uppnås. Det kräver bl.a. att ledningssystemet stärker ledningens möjligheter att överblicka risker, samt ger information om behovet av säkerhetsåtgärder och kostnaderna för säkerhetsarbetet. Den i granskningen använda LIS-standarden innehåller enligt Riksrevisionens bedömning de viktigaste kraven på ett sådant ledningssystem. Det är dock ledningens ansvar att bestämma hur ledningssystemet ska utformas.

Vissa delar av Migrationsverkets ledningssystem för informationssäkerhet finns redan på plats, om än inte fullständigt utvecklade. Det gäller ansvarsfördelning, tekniska skyddsåtgärder och styrdokument för säkerhetsarbetet. Granskningen visar dock att i vissa andra delar har ledningens arbete med informationssäkerheten brister. Det gäller kontrollmiljön, riskanalys, kontrollfunktioner, uppföljning och utbildning. Dessa brister påverkar i sin tur ledningens möjlighet att uppnå eftersträvad informationssäkerhet.

Bristerna avser väsentliga punkter i ledningssystemet och Riksrevisionen bedömer därför att Migrationsverket, utifrån gängse normer, inte fullt ut arbetar systematiskt med sitt ledningssystem för informationssäkerhet.

Rekommendationer

De brister som Migrationsverket framförallt bör åtgärda är följande:

- *Bristande möjlighet att överblicka risker och skyddsvärda informationstillgångar*

I ledningens engagemang för säkerhetsfrågor saknas ett mer systematiskt angreppssätt när det gäller prioriteringar och uppföljning. Ledningens kontrollmiljö har brister som främst rör de förutsättningar

som ledningen skapat för informationssäkerhetsarbetet. Detta innebär att vikten av dessa frågor inte beaktats i tillräcklig utsträckning.

Migrationsverket har för närvarande ingen samlad riskanalys som kan utgöra grund för prioritering och effektivt införande av skyddsåtgärder på informationssäkerhetsområdet. Trots att Migrationsverket i interna beslut fastställt att analyser ska genomföras har detta inte gjorts vare sig på lokal nivå eller gemensamt för verket.

Det finns heller inte någon heltäckande informationsklassificering, vilket bland annat exemplifieras av att Migrationsverket inte klassificerar tillgångarna utifrån tillgänglighetskrav trots att det under granskningen framkommit att delar av verksamheten har mycket höga krav på tillgänglighet till informationsresurserna. Någon aktuell samlad förteckning över verkets informationstillgångar har heller inte presenterats för Riksrevisionen.

- *Brister i ledningens kontrollfunktioner samt införda säkerhetsåtgärder*

Migrationsverket har till stor del beslutat om och infört styrdokument som handlar om informationssäkerheten. I dessa dokument behandlas i allt väsentligt vilka kontrollfunktioner som ska finnas och vem som har ansvar för att de utförs. Flera brister har dock iakttagits i utförandet av kontrollfunktionerna.

Kontinuitetsplaner och åtgärdsplaner saknas helt trots att de ska upprättas enligt det interna regelverket. Migrationsverket saknar också en fastställd rutin för vilka incidenter som ska rapporteras till ledningen.

Vid tidigare granskningar av Migrationsverket som utförts av den årliga revisionen har brister identifierats i behörighetssystemet samt i uppföljningen av att behörigheterna är anpassade efter personalens arbetsuppgifter.

Migrationsverkets granskning av loggar utförs i hög grad efter det att verket fått indikationer på problem från andra källor, vilket ger sämre förutsättningar att upptäcka eventuellt missbruk av information eller felaktigheter i systemen. Att loggranskning faktiskt sker är svårt att verifiera eftersom det inte finns någon dokumentation av utförda granskningar.

- *Brister i utbildning och uppföljning*

Migrationsverket saknar en systematisk plan för utbildning i informationssäkerhetsfrågor för såväl verksamhetsansvariga chefer som för övrig personal. Migrationsverket har därmed inte säkerställt att personal, ansvariga chefer och systemägare ges tillräcklig information om de risker och hot som finns inom informationssäkerhetsområdet. Detta medför en ökad risk att berörda personalkategorier inte kan

fullgöra det ansvar som delegerats till dem avseende informationssäkerheten.

Enligt Riksrevisionens bedömning saknar Migrationsverket en väl utvecklad strategi för hur önskad kvalitet i verkets ledningssystem ska uppnås. En grundläggande brist i informationssäkerhetsarbetet är avsaknaden av såväl klassificering och aktuell förteckning av informationstillgångar som av riskanalys och åtgärdsplaner. Det medför att Migrationsverket inte kan ge en samlad bild av om de befintliga säkerhetsåtgärderna, och uppföljningen av dessa, tillsammans ger ett fullgott skydd. Sammantaget är Riksrevisionens bedömning att uppföljningen av ledningssystemet brister i systematik och regelbundenhet, vilket medför en ökad risk för att informationssäkerhetsincidenter inte kan förebyggas, upptäckas och åtgärdas på ett effektivt sätt.

1 Inledning

1.1 Bakgrund, syfte och revisionsfrågor

1.1.1 Bakgrund

Under 2005-2006 har Riksrevisionen granskat informationssäkerheten på tio statliga myndigheter.[1] Denna granskning avser Migrationsverkets informationssäkerhet.

Informationssäkerhet[2] omfattar

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

Informationssäkerheten är 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 förstärka skyddet mot de risker som uppstår.

---

[1] Sex granskningar har gjorts utifrån den presenterade metoden: Sjöfartsverket, Statens Pensionsverk, Försäkringskassan, Lantmäteriverket, Migrationsverket och Arbetsmarknadsverket. Metoden har i vissa delar tillämpats i ytterligare fyra granskningar, men dessa granskningar 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 obehöriga 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 angripare gjort en utförlig kartläggning av organisationens system, dvs. att obehöriga 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, trojaner m.m.

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 verksledningen 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 dock medveten om att det hos Migrationsverket 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[5]. 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 Migrationsverket, utifrån gängse normer, systematiskt med sin informationssäkerhet?

1.2 Bedömningskriterier

I bedömningen av Migrationsverkets styrning och ledning av informationssäkerhetsarbetet har Riksrevisionen utgått från ett flertal normer och standarder[6]. 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[7]) innehåller riktlinjer som enligt standarden ”bör betraktas som ett underlag för att utveckla organisationsspecifika riktlinjer. Allt som nämns i LIS-standarden är kanske inte

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

[6] 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.

[7] I rapporten används begreppet LIS eller 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.

tillämpligt. Ytterligare åtgärder, som inte anges i denna standard, kan också vara nödvändiga."[8]. Samtidigt utgör standarden "en gemensam grund för i princip alla organisationer."[9].

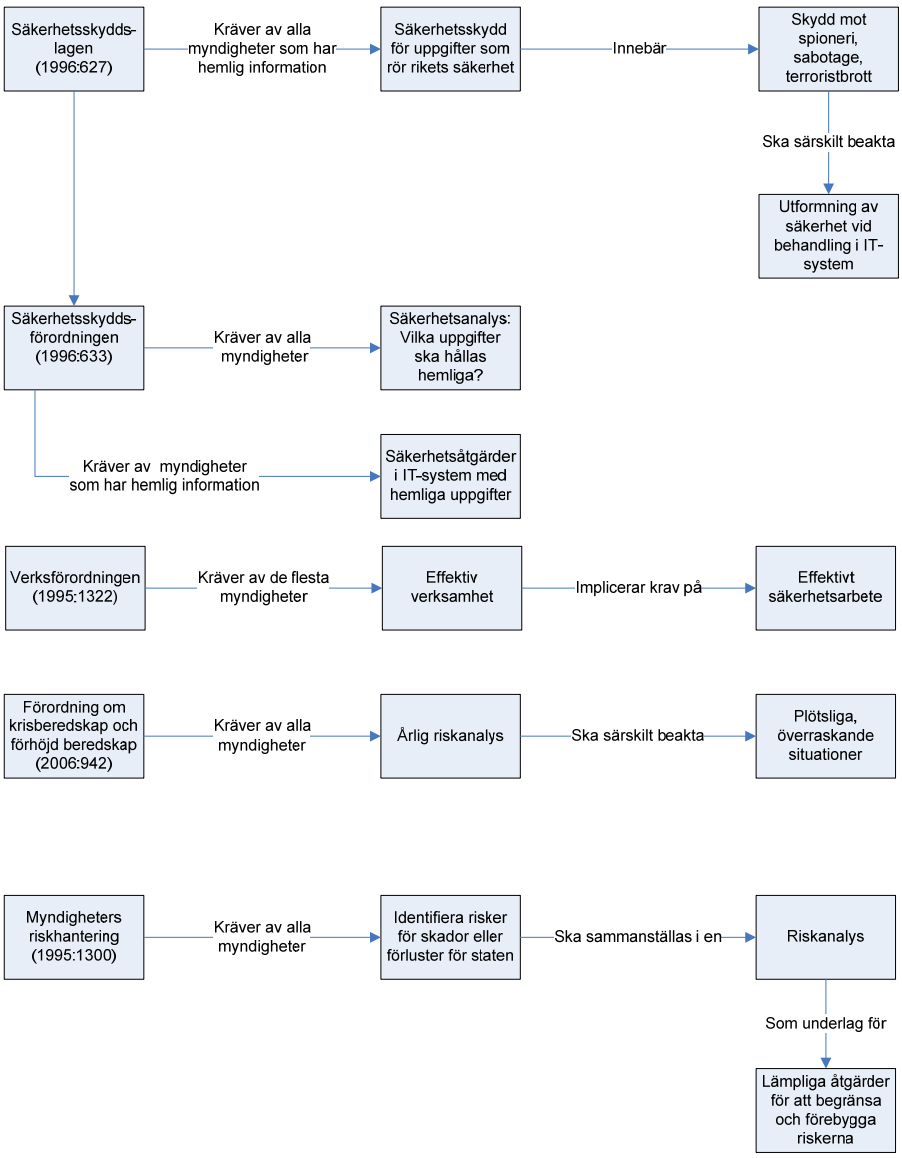
För Riksrevisionens beslut har följande faktorer haft betydelse:

- LIS-standarden är den mest 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 visat sig vara stabila. Standarden har efter tio år nu uppdaterats beträffande sin disposition men den är innehållsmässigt intakt.

1.2.1 *Översikt över lagar och förordningar som berör informationssäkerhet*

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]).

[8] SS-ISO/IEC 17799 s. 10.
[9] 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 förmågan att hantera mycket allvarliga situationer inom myndighetens ansvarsområde (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 som skydd mot spionerі, terroristbrott m.m. som kan hota rikets säkerhet (5 § säkerhetsskyddslagen) och som förebygger brister i informationssäkerhet som avser hemlig information (7 och 9 §§ säkerhetsskyddslagen)
- krav på *särskilda säkerhetsåtgärder* – behörighetskontrollsystem, händelseloggning, samråd med säkerhetsmyndigheterna i vissa fall, godkänd kryptering, inventering av hemliga handlingar – för de IT-system som används för hemlig information (12 § säkerhetsskyddsförordningen). Regeringen har här alltså funnit anledning att formulera relativt konkreta krav på dessa myndigheters 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 enbart till 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 det säkerhetsarbete 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 7 § verksförordningen – 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[10]. Granskningsprogrammet har behandlats i seminarier med Swedish Standards Institute, Krisberedskapsmyndigheten, 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 ovannämnda 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.

[10] 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. Kapitel 3-7 i Riksrevisionens rapport anknyter till dessa beståndsdelar.

1.3 Metoder och tillvägagångssätt i granskningen

Granskningen har genomförts på följande sätt:

- Migrationsverket valdes ut för granskning på grund av att verket hanterar stora mängder integritetskänsliga personuppgifter. Riksrevisionen hade alltså ingen information om 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. I samband med introduktionen av granskningen genomfördes en första översiktlig intervju med biträdande säkerhetschefen, vilken inkluderade diskussion om förekomst av dokument.
- Myndigheten har därefter fått besvara ett frågeformulär (dvs. en självutvärderingsenkät) om myndighetens syn på sin verksamhet och behovet av informationssäkerhet. Myndigheten har 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 s.k. nyckeldokument som Riksrevisionen behövt för sin granskning. Myndigheten har sedan översänt dessa. Myndigheten har gjort en egen bedömning av vilka av dess dokument som motsvarar Riksrevisionens beskrivningar och som tillsammans ger en rättvisande bild av myndighetens ledningssystem för informationssäkerhet.
- Efter det att Riksrevisionen gått igenom dokumenten har företrädare för myndigheten blivit intervjuade[11] med stöd av granskningsprogrammets intervjufrågor. 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 faktagranskat utkastet till revisionsrapport.

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.

[11] GD, ÖD, verksamhetsområdeschefer, biträdande säkerhetschef, rättschef, IT-chef, IT- och säkerhetsexpert, drift-och supportchef, systemutvecklingschef samt systemförvaltningschef.

Ett annat ord som används är ”tillräcklig”. Det är en bedömning som Riksrevisionen gör av hur långt Migrationsverket kommit i förhållande till Riksrevisionens tolkning[12] 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 Migrationsverket i t.ex. 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.

[12] 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 Migrationsverket och informationssäkerheten

2.1 Migrationsverkets verksamhet m.m.

Migrationsverket (i fortsättningen även kallat verket) är Sveriges centrala förvaltningsmyndighet för verksamhet inom migrationsområdet och ansvarar för tillstånd eller visum för besök, tillstånd för bosättning i Sverige, asylprocessen från ansökan till uppehållstillstånd eller självmant återvändande, medborgarskap, stöd för frivillig återvandring samt internationellt arbete inom EU, FN:s flyktingorgan UNHCR och andra samverkansorgan. Migrationsverket ansvarar även för anläggningsboenden för de asylsökande som inte väljer eget boende. Migrationsverket administrerar även bidrag till asylsökande samt ersättningar till landsting och kommuner m.fl. enligt bl.a. sjukvårdsförordningen och asylersättningsförordningen. Verksamheten omfattar dessutom omprövning av utlänningsärenden och medborgarskapsärenden. Verket hade per 2005-12-31 ca 3 150 anställda. Totalt finns verksamhet på runt 40-talet orter. Verksledningen (generaldirektör, överdirektör och rättschef) är stationerade i Norrköping. Den rådgivande ledningsgruppen består, förutom verksledningen, av verksamhetscheferna för verkets sex verksamhetsområden.

Under 2005 var utgifterna ca 4,4 miljarder kronor, varav ca 3,8 miljarder avsåg transfereringar och 0,6 miljarder prövningsverksamheten.

Migrationsverket finansieras främst genom anslag, men vissa avgifts- och bidragsintäkter förekommer också.

De förvaltningsrättsliga föreskrifter som reglerar verkets verksamhet är förutom regleringsbrevet och instruktionen (Förordning (2004:294) med instruktion för Migrationsverket) i huvudsak:

- Utlänningslagen (2005:716)
- Utlänningsförordningen (2006:97)
- Lagen (2001:82) om svenskt medborgarskap
- Dublinförordningen (EU - förordning 343/2003)
- Lag om mottagande av asylsökande (1994:137)
- Förvaltningslagen (1986:223)
- Sekretesslagen (1980:100)
- Personuppgiftslagen (1998:204)
- Lagen om offentlig upphandling (1992:1528)

- Arkivlagen (1990:782)

Därutöver finns föreskrifter (MIGRFS) som Migrationsverket utfärdar.

2.2 Informationstillgångarna och Migrationsverkets bedömning av säkerheten för dessa

Inslaget av IT-stöd i Migrationsverkets processer är betydande, och Migrationsverket är starkt IT-beroende. Det ställs stora krav på att den information som finns i Migrationsverkets informationssystem är säkerställd. Med detta menas att informationens riktighet, tillgänglighet, sekretess samt spårbarhet är skyddad. Den information som lagras i Migrationsverkets IT-system är ofta sekretessbelagd, informationen är också ofta av känslig natur för den enskilde samt för rikets säkerhet. Enligt verkets svar på Riksrevisionens enkät betraktas informationssäkerhet som en viktig ledningsfråga som Migrationsverket under en tid inte haft möjlighet att i önskvärd utsträckning uppmärksamma.

Flera faktorer påverkar Migrationsverkets bedömning av informationssäkerhetens betydelse i verksamheten. Migrationsverket framhåller i sitt enkätsvar att storleken hos betalningsströmmarna i verksamheten, omfattningen av IT-beroende, volymen integritetskänslig information, volymen sekretesskänslig information, volymen ärenden som behandlas samt vikten av kontinuitet i verksamheten som särskilt betydelsefulla faktorer för utformningen av arbetet med informations- och IT-säkerhet. Sammantaget anser Migrationsverket enligt sitt enkätsvar att verket har en informationssäkerhet som är behäftad med vissa mindre brister.

2.2.1 Viktiga IT-system hos migrationsverket

Migrationsverkets IT-system finns i huvudsak i Norrköping där driften sker. För driften av verkets IT-system har verket anlitat en underleverantör. Brister i systemens säkerhet kan leda till att sekretessbelagd eller känslig information kan hamna i orätta händer. En viktig del i informationssäkerheten är en korrekt hantering av bl.a. personuppgifter; fel vid handläggningen av asyl-, tillstånds- och medborgarskapsärenden kan leda till att fel beslut fattas. Ett positivt beslut om asyl samt beslut om medborgarskap kan inte återkallas oavsett om beslutet har fattats på fel grunder. Brister i förmågan att skydda informationstillgångarna kan också äventyra allmänhetens förtroende för Migrationsverket.

För att ge läsaren en bild av vilka IT-system som finns hos Migrationsverket anges här några av de viktigaste:

- Wilma som främst används till att handlägga ärenden inom tillståndsprövningsverksamheten, dvs. för beslut i ärenden rörande visum, uppehållstillstånd, arbetstillstånd m.m. Wilma hanterar även den s.k. förvaltningsprocessen, där ärenden rörande asyl, tillstånd och medborgarskap omprövas. Även Polisen och utlandsmyndigheterna har tillgång till Wilma.
- Skapa som används för kvalitetssäkring och dokumentation av asylprocessens handläggningsrutiner och beslut.
- Stamm som används i mottagningsprocessen för bosättning och bidragsutbetalningar till asylsökande. Systemet används även för handläggning och beslut i medborgarskapsprocessen.
- Centrala utlänningsdatabasen, vanligen kallad CUD, är egentligen ett begrepp som omfattar de databaser som Migrationsverket har där data om verkets utlänningsärenden finns registrerade.

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

3.2 Iakttagelser

Migrationsverkets val av organisation för IT-verksamheten grundas till stor del på Statskontorets rapport ”Granskning av Migrationsverkets IT-verksamhet (2002/524-5)”. Statskontoret utförde denna granskning på regeringens uppdrag. Dock har Statskontorets förslag inte implementerats fullt ut. Först

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

under 2005 tillträdde nuvarande IT-chef. I den nya IT-enheten har roller som IT-chef, drift- och supportchef, systemutvecklingschef och systemförvaltningschef skapats. Dessutom finns tjänster som IT-säkerhetsexpert samt en tjänst för projekt och metodansvar i den nya organisationen.

Statskontorets förslag var främst följande:

- De övergripande målen för IT-verksamheten bör preciseras med utgångspunkt i målen för verksamheten i stort.
- En resurs- och kompetensmässigt stärkt central IT-funktion bör inrättas med övergripande ansvar för bl.a. strategisk planering, normgivning, styrning och uppföljning, samverkan/samordning och andra verksgemensamma frågor.
- Ett stärkt systemägarskap, en utvecklad beställarkapacitet och en förstärkt central IT-funktion lägger grunden för en väl avvägd och effektiv användning av externa resurser och därmed ett minskat leverantörsberoende.
- Balansen och kompetensmixen mellan egen regi/entreprenad bör ses över med inriktningen att minska nuvarande starka leverantörsberoende.
- Migrationsverkets förmåga att med egen kompetens agera som ”ägare” samt kompetens och rutiner rörande projektstyrning, projektadministration och resultatuppföljning bör förstärkas.
- För att undvika förseningar bör – som ett första steg – en IT-chef rekryteras med den inledande uppgiften att i samverkan med övriga verksamhets- och utvecklingsansvariga planera och organisera förändringsarbetet.

Migrationsverket har utarbetat vissa styrdokument för arbetet med informationssäkerhet: **informationssäkerhetspolicy**, daterad 2003-02-01, och instruktion om IT-säkerhet vid Migrationsverket, daterad 2004-02-03. Dessa två dokument är dock inte helt uppdaterade i och med den organisationsförändring som genomfördes per 2005-01-01. Arbetsordningen, daterad 2006-04-05, innehåller uppgifter om organisation och ansvarsområden. Alla tre dokumenten är beslutade av generaldirektören.

Av **informationssäkerhetspolicyn** framgår vad informationssäkerhet är, att verket ska använda den s.k. LIS-standarden ISO/IEC 17799 i informationssäkerhetsarbetet, vilka mål verket har med informationssäkerhetsarbetet samt övergripande information om hur arbetet ska bedrivas. Som medel för att nå målen anges att verket ska avdela resurser för att systematiskt genomföra riskbedömningar och konsekvensanalyser, ta fram riktlinjer och handlingsplaner, genomföra informationssäkerhetshöjande åtgärder samt utbildnings- och informationsinsatser.

I instruktion om IT-säkerhet vid Migrationsverket finns mer detaljerad information om krav på utrustning, program samt kontroller. Av instruktionen framgår också att systemägarna ansvarar för att varje systems sårbarhet fortlöpande analyseras. Systemägarna ansvarar för informationssäkerheten i de egna systemen. Systemansvariga genomför denna analys på de system eller delsystem som de ansvarar för.

Verksamhetsansvariga ansvarar inom sitt område för att IT-stödet Analyseras på samma vis. I sårbarhetsanalyserna ska nuvarande och framtida hot mot IT-verksamheten identifieras, sannolikhetsbedömas och konsekvensbedömas. Vid brister ska förslag till åtgärder tas fram. Sårbarhetsanalyserna ska dokumenteras, och resultatet av analysen ska ingå i den ordinarie verksamhetsplanen. Verksamhetsansvariga ansvarar för att deras personal får kunskap om säkerhetspolicy och gällande regelverk samt för säkerhetsarbetet inom sitt ansvarsområde.

Enligt arbetsordningen ansvarar säkerhetsenheten för säkerhets- och totalförsvarsfrågor. Den ska även bereda handbokstexter inom ansvarsområdet. Säkerhetschefen och biträdande säkerhetschefen är i säkerhetsfrågor direkt underställda generaldirektören. Administrativt sett ingår säkerhetsenheten i verksamhetsområdet förvaltning och internationella frågor.

IT-enheten ansvarar för att åtgärda brister i IT-systemen och infrastrukturen. Enligt intervjuer initieras åtgärderna oftast tillsammans med säkerhetsenheten.

LIS-standarden anger att ett uttryck för ledningens **engagemang** för informationssäkerhet är att ledningen preciserar ansvar och aktiviteter för att få nödvändig överblick över informationstillgångarna, vilket möjliggör en riktig prioritering av skydds- och säkerhetsåtgärder. Prioriteringen ska enligt standarden baseras på en riskanalys. För Migrationsverkets del finner Riksrevisionen att detta ansvar är utpekat vad gäller olika system och enheter, men det finns ingen utpekad funktion som ansvarar för att en samlad övergripande sårbarhetsanalys/riskanalys upprättas för hela verket. Någon riskanalys i LIS-standardens mening har inte presenterats för Riksrevisionen, ej heller riskanalyser för enskilda system och enheter. Vid intervjuerna framkom att det inte upprättats några riskanalyser.

Av den självutvärderingsenkät Migrationsverket besvarat samt av intervjuerna framgår att verket främst använt LIS-standarden som ett ”smörgåsbord”. Migrationsverket har valt bort vissa krav som rör dokumentation av ledningssystemet, reglering av informationssäkerhetsfrågor i anställningsavtal, e-handel, säkerhet i delade nätverk samt modifieringar av programpaket. Som nämns ovan finns det brister i dokumentationen av Migrationsverkets ledningssystem, se även följande kapitel. Det verktyg verket använder i syfte att analysera och upptäcka bristerna inom informationssäkerhetsområdet är SBA Check.

Någon beslutad och finansierad åtgärdsplan baserad på den bristrapport som SBA Check ger upphov till finns inte. Migrationsverket anger att de identifierade bristerna till viss del har åtgärdats. Rörande de granskningar Försvarets radioanstalt (FRA) genomfört på Migrationsverkets uppdrag finns det heller inte någon beslutad och finansierad åtgärdsplan. Bristen på beslutade och finansierade åtgärdsplaner kan leda till att mer resurskrävande åtgärder inte genomförs. Ett exempel är de brister avseende reservkraft som finns, bristerna har lett till att IT-systemen inte varit tillgängliga vid några tillfällen. Ytterligare en risk är att de mest relevanta åtgärderna inte valts eller inte väljs eftersom ledningen inte tagit ställning till och rangordnat riskerna sinsemellan i t.ex. en riskanalys. Utöver **informationssäkerhetspolicyn**, instruktion för informationssäkerhet vid Migrationsverket samt arbetsordningen finns det få dokument upprättade rörande informationssäkerheten. Förutom att en dokumenterad riskanalys saknas, så saknas också bl.a. avbrottsplan, hotbildsanalys och dokumenterade systemsäkerhetsplaner.

Krav på informationssäkerhet har hittills inte behandlats som funktionalitetskrav vid systemutveckling eller beaktats vid kontroller innan system och rutiner tagits i drift. Hanteringen av säkerhetsfrågorna har hittills inte varit en integrerad del i processen för systemutveckling. Verket beslutade den 10 oktober 2006 om införande av projektstyrningsmetoden PROPS, där säkerhetsfrågorna kan hanteras som en integrerad del av utvecklingsarbetet.

Övriga iakttagelser är att Migrationsverket inte har någon särskild budget för arbetet med informationssäkerhet, varför det är svårt att bedöma hur mycket resurser som finns tillgängligt för detta ändamål. Något som också framkom vid intervjuerna var att verket anses vara bra på snabba anpassningar i och av verksamheten men sämre på uppföljning, dokumentation samt på att upprätthålla rutiner. Under intervjuerna framkom att kraven på tillgänglighet och säkerhet i IT-systemen upplevs som otydliga. I flera intervjuer har även påpekats att vissa IT-system anses vara svåra för användarna att använda, vilket kan leda till fel i handläggningen.

I Regeringskansliets generella IT-plattform och IT-stöd för utlandsmyndigheterna ingår inte stöd rörande Wilma. IT-stöd rörande Wilma står Migrationsverket för. Migrationsverkets säkerhetsenhet besöker utlandsmyndigheterna (för närvarande ca 2 st/år) för att kontrollera säkerheten rörande verkets system. Dessa besök rapporteras skriftligt och redovisas för Utrikesdepartementet och Migrationsverkets generaldirektör.

Ledningens uppföljning är en annan viktig del av **engagemanget** för informationssäkerheten. Ledningens uppföljning bygger på incidentrapportering och incidenthantering, dvs. hantering av uppkomna brister i verksamhetens säkerhet. På vilket sätt ledningen ska följa upp det delegerade ansvaret för informationssäkerheten har inte tydliggjorts i styrdokumenten,

vilket är en brist (mer om detta i kapitel 7). Det som saknas är en systematisk uppföljning utöver denna rapportering och hantering.

Beträffande ledningens **förtrogenhet** med informationssäkerhetsarbetets ledningsfrågor kan det dessutom konstateras att ledningsgruppen inte genomgått någon särskild utbildning i informationssäkerhet. Resultatet av den genomgång av informationssäkerheten som gjorts med hjälp av SBA Check förefaller ledningen inte känna till. Detsamma gäller rapporterna från FRA. Några riskanalyser, avbrottsplaner eller åtgärdsplaner har ledningen inte efterfrågat, enligt vad som framkommit under intervjuer och dokumentstudier.

3.3 Bedömning

De i avsnitt 3.2 beskrivna bristerna vad gäller övergripande riskanalys samt bristen på dokumentation medför att ledningens möjlighet till överblick försvåras. Verket har beslutat om regler för informationssäkerhetsarbetet i bl.a. informationssäkerhetspolicyn, men denna policy följs inte fullt ut vilket framgår av iakttagelserna ovan. Vem som ansvarar för vad i informationssäkerhetsarbetet är också otydligt. Bristen på riskanalyser samt utbildning innebär att verket saknar viktiga komponenter i sitt ledningssystem. Det faktum att verket ansvarar för IT-systemet Wilma, där arbete även utförs av personal annan än verkets egen samt i lokaler andra än verkets egna kan innebära risker som verket kan få svårt att överblicka och kontrollera.

Krav på informationssäkerhet har hittills inte behandlats som funktionalitetskrav vid systemutveckling, vilket medför säkerhetsrisker samt risk för avsevärda fördyringar för verket när system behöver vidareutvecklas eller när helt nya system behöver tas fram.

Ledningen har inte skapat tillräckliga förutsättningar för informationssäkerhetsarbetet. I ledningens engagemang för säkerhetsfrågorna saknas ett mer systematiskt/strukturerat angreppssätt när det gäller prioriteringar och uppföljning. Riksrevisionen bedömer därför att de iakttagna bristerna i kontrollmiljön medför att ledningen inte haft möjlighet att säkerställa att de gjort en korrekt prioritering av skydds- och säkerhetsåtgärder. De brister i ledningssystemet för informationssäkerhet som angetts ovan kan påverka informationssäkerheten 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[14]. 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**[15]. Riskanalysen bör uppdateras årligen, och däremellan vid behov.

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

Det bör finnas en tydlig och uppföljningsbar **åtgärdsplan** som förtecknar beslutade säkerhetsåtgärder[16] 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

---

[14] 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.

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

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

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

4.2 Iakttagelser

Migrationsverket har i såväl informationssäkerhetspolicy som instruktion om informationssäkerhet, beslutat om regler för arbetet med att analysera informationssäkerhetsrisker. Enligt verkets instruktion om informationssäkerhet ska **sårbarhetsanalyser** göras fortlöpande. Systemägaren ansvarar för att detta genomförs avseende respektive systems sårbarhet, och verksamhetsansvariga ansvarar inom sitt område för att IT-stödet analyseras på samma vis. I sårbarhetsanalyserna ska nuvarande och framtida hot mot IT-verksamheten identifieras, sannolikhetsbedömas och konsekvensbedömas.

Vid brister ska förslag till åtgärder tas fram. Sårbarhetsanalyserna ska dokumenteras, och resultatet av analyserna ska ingå i den ordinarie verksamhetsplanen. Brister som inte åtgärdas ska rapporteras till informationssäkerhetssamordnaren.

Som redan påpekats i denna rapport finns det inget tydligt utpekat ansvar för att upprätta eller sammanställa en **samlad risk- eller sårbarhetsanalys** beträffande informationssäkerhet för Migrationsverket. Den enda riskanalys som presenterats av Migrationsverket under granskningen är en mycket övergripande analys som upprättats i syfte att uppfylla kraven i förordningen (1995:1300) om statliga myndigheters riskhantering. Denna analys berör endast i vissa begränsade delar informationssäkerhetsområdet. Intervjuer med verksamhetsansvariga visar att det i övrigt inte genomförts några dokumenterade risk- eller sårbarhetsanalyser i verksamheten, av den typ som beslutats i instruktionen om informationssäkerhet. Med andra ord finns det, utöver den mycket övergripande riskanalysen som nämnts ovan, inte någon överblick över risknivån i de olika delarna av verksamheten.

Driften av verkets IT-verksamhet är utlagd på underleverantör. Någon samlad riskanalys avseende denna verksamhet finns enligt intervjuerna inte, utan riskanalyser genomförs i anslutning till enskilda projekt och uppdrag. Dock anger verket att dessa analyser inte alltid är dokumenterade.

Migrationsverket har idag ingen fastställd **metod** för riskanalys. Därför finns det i dagsläget inte heller förutsättningar för att genomföra analyser på ett likartat sätt i organisationen, t.ex. avseende likartad grund för analys och värdering av olika risker.

Instruktion för informationsklassificering har beslutats av generaldirektören. Instruktionen är från 1998 och har inte uppdaterats sedan dess. Den

omfattar dessutom bara sekretessklassificering av ärenden samt uppgifter om anställda. I dokumentet anges att övrig info vid Migrationsverket inte är integritetskänslig och därför ej fordrar särskilda skyddsåtgärder. Detta innebär att informationstillgångarna vid verket inte klassificeras utifrån t.ex. tillgänglighetskrav, trots att intervjuer visat att delar av verksamheten har mycket höga krav på tillgänglighet till information och applikationer. Intervjuerna visar att det i dag uppfattas som otydligt vem som har ansvaret för att klassificering faktiskt genomförs. Enligt instruktionen ansvarar den som upprättar en handling eller vidarebefordrar information för att alltid ta ställning till hur informationen ska klassas och transporteras.

Vid granskningstillfället har en aktuell samlad **förteckning** över samtliga Migrationsverkets informationstillgångar inte kunnat presenteras. Intervjuerna visar att det är oklart vem i organisationen som ansvarar för upprättande av en sådan förteckning.

Incidenter med påverkan på informationssäkerheten ska, enligt verkets instruktion om informationssäkerhet, rapporteras till säkerhetsfunktionen vid huvudkontoret. Anvisningar för hur rapporteringen ska gå till finns tillgängliga på intranätet. Det finns dock inga definitioner av vilken typ av **incidenter** som ska rapporteras. Det finns heller inte någon fastställd rutin för rapportering till ledningen. Vid intervjuer har angetts att ärenden som avser säkerhetshot eller ”allvarliga avbrott” rapporteras till verksledningen. Ansvaret för hantering av incidenter finns endast muntligt uttryckt och har inte formaliserats. Detta område tas även upp i kapitel 5.2.

Enligt intervjuerna finns inte någon samlad **åtgärdsplan** för hantering av risker i verksamheten, utan dessa hanteras allteftersom de upptäcks. Därmed finns en risk att åtgärder inte vidtas utifrån en övergripande prioriteringsordning och att verket inte bedriver säkerhetsarbetet på ett kostnadseffektivt sätt (se vidare i kapitel 7).

4.3 Bedömning

De uppgifter som Migrationsverket lämnat inför granskningen samt de genomförda intervjuerna visar att det interna regelverket avseende risk- och sårbarhetsanalyser inte efterlevs. Den enda analys som presenterats är en mycket övergripande analys, som dock inte i någon större omfattning bygger på information som inhämtats från organisationen.

Riksrevisionen kan vidare konstatera brister i arbetet med att såväl klassificera Migrationsverkets informationstillgångar som förteckna dessa. Riksrevisionens bedömning är att detta till viss del är ett resultat av oklarheter rörande vilka ansvarsförhållanden som gäller för att utföra dessa arbetsuppgifter.

Verksledning och verksamhetschefer saknar enligt Riksrevisionens bedömning tillräckligt metodstöd för att skapa en rättvisande och överblickbar bild över riskläget i olika delar av verksamheten. Denna brist på överblick medför enligt Riksrevisionens bedömning svårigheter för verksledningen att avgöra om beslutade säkerhetsåtgärder är i linje med gällande regelverk och riktlinjer. Verksledningen har enligt Riksrevisionens bedömning inte heller möjlighet att överblicka utestående[17] risker och hur hanteringen av dessa risker utvecklas över tiden, då någon form av formell åtgärdsplan inte finns.

Riksrevisionen bedömer att de brister som framkommit ovan innebär att Migrationsverket saknar en sammanhängande, systematisk och dokumenterad process för förteckning, klassificering och riskbedömning av sina informationstillgångar. Dessa brister kan påverka kvaliteten i ledningsarbetet inom informationssäkerhetsområdet. Sammantaget bedöms därför Migrationsverkets arbete med att analysera och bedöma risker rörande informationssäkerheten ha flera betydande brister. Dessa brister i ledningssystemet för informationssäkerhet kan påverka informationssäkerheten negativt.

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

5 Ledningens kontrollfunktioner och införda 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, loggningsförfaranden m.m. Kontrollfunktionerna utgör sammantagna en väsentlig del av myndighetens ledningssystem.

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.

Ledningssystemet bör normalt ha följande **omfattning** när det gäller komponenter[18]:

- 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,
- åtkomstpolicy19,
- process för säkerhetskopiering av all verksamhetskritisk information,

[18] 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.

[19] Policy som reglerar åtkomst till informationstillgångar.

- process för styrning av utveckling/förändringar i IT-miljö, IT-system och bemanning,
- tekniska säkerhetsåtgärder (behörighetskontrollsystem, virusskydd, brandväggar m.m.),
- processer för att kontrollera efterlevnaden av det regelverk för upprätthållande av informationssäkerhet som bl.a. ovannämnda policykomponenter tillsammans bildar,
- en till all personal kommunicerad skriftlig beskrivning av roller[20] 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**[21] inom aktuellt område. De bör vidare vara väl **införda** i verksamheterna. Komponenterna bör tillsammans utgöra en lämpligt utformad **helhet** genom sina inbördes samband samt utgöra en väl integrerad del i myndighetens (totala) ledningssystem.

5.2 Iakttagelser

Granskningen visar att Migrationsverket har delar av ett ledningssystem med **dokumenterade och beslutade komponenter**. De delar som införts omfattar övergripande policydokument och riktlinjer, ansvarsfördelning och organisation, rutinbeskrivningar för vissa delar av säkerhetsarbetet samt ett flertal tekniska säkerhetsåtgärder som ingår i verkets IT-infrastruktur.

Migrationsverket har som tidigare nämnts en beslutad informationssäkerhetspolicy och en instruktion om informationssäkerhet vid Migrationsverket. Instruktionen innehåller mer preciserade riktlinjer för IT-systemen och IT-produkter och behandlar sårbarhetsanalyser, förändringar i nätverket, ansvarsområden, avbrottsplaner för IT-system, behörigheter, incidentrapportering, användning av Internet, krav på IT-utrustning, distansarbete, krav på program, säkerhetskopiering, användning av e-post och kommunikation, radering av IT-medier som innehåller hemlig information samt krav på lokaler där IT-utrustning förvaras. Dokumenten finns tillgängliga i Migrationsverkets intranät.

---

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

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

I Migrationsverkets arbetsordning är det fastställt att säkerhetschefen ansvarar för säkerhetsskyddet vid Migrationsverket enligt säkerhetsskyddsförordningen (1996:633). Vidare framgår av informationssäkerhetspolicyn att säkerhetsenheten har ett särskilt ansvar för informationssäkerhetsfrågor. Säkerhetschefen har ett övergripande ansvar för uppföljning av informationssäkerheten och kontroll av efterlevnaden. Säkerhetschefen och biträdande säkerhetschefen är i säkerhetsfrågor direkt underställda generaldirektören.

Som tidigare nämnts i kapitel 3 har Migrationsverket valt bort vissa krav som rör dokumentation av sitt ledningssystem, reglering av informationssäkerhetsfrågor i anställningsavtal, e-handel, säkerhet i delade nätverk samt modifieringar av programpaket.

Viktigare tekniska säkerhetsåtgärder som finns är reservanläggning för IT-drift (alternativ datorhall), behörighetskontrollsystem, säkerhetskopiering av information, kryptering samt helpdesk.

Det finns dock brister i Migrationsverkets ledningssystem för informationssäkerhet, vilket leder till att det inte fungerar utifrån **best practice**.

Migrationsverket har många verksamhetsområden som alla är beroende av informationssäkerhet. Sekretess, tillgänglighet och riktighet krävs inom alla verksamhetsområden och har i intervjuerna nämnts som särskilt viktiga inom verksamhetsområdena asyl, besök och bosättning samt medborgarskap. Samtliga intervjuade verksamhetschefer anser att frågan om informationssäkerhet är mycket viktig. Enligt verkets beslutade informationssäkerhetspolicy ska informationssäkerheten ingå som en naturlig del av verkets verksamhetsplanering. Ändå har Migrationsverket inga uttryckliga mål för informationssäkerhetsarbetet som kan kopplas till de enskilda verksamhetsområdena.

För att analysera och upptäcka brister inom informationssäkerhetsområdet använder sig Migrationsverket av verktyget SBA check. Denna analys mynnar ut i en bristrapport. Enligt intervjuer används bristrapporten som dokumentation och bristerna åtgärdas i den takt som är möjlig. Det finns ingen fastställd ordning för hur bristrapporten ska kommuniceras till ledningsgruppen. Någon beslutad och finansierad åtgärdsplan finns inte upprättad för de brister som identifierats.

Migrationsverket har löpande fått sin intrångssäkerhet prövad genom s.k. penetrationstester utförda av FRA. FRA:s slutsatser har enligt vad som framkommit i intervjuer inte heller kommunicerats till ledningsgruppen. De brister som framkommit genom dessa analyser har inte heller resulterat i någon beslutad åtgärdsplan, och FRA har ifrågasatt varför återkommande brister inte har åtgärdats i enlighet med tidigare rekommendationer.

Migrationsverket har ingen formell struktur eller fastställd rutin för vilka incidenter som ska rapporteras till ledningen. I intervjuer har framkommit att det finns oklarheter i vad som efterfrågas av ledningen. Ledningsgruppen

har inte heller på ett tydligt sätt definierat vilken typ av information som ska rapporteras till dem. I vissa intervjuer har angetts att ärenden som avser säkerhetshot eller ”allvarliga avbrott” rapporteras till verksledningen. I den rutin som tillämpas för incidentrapportering till helpdesk ska användarstöden ute i organisationen rapportera in incidenter. Vad som kan utgöra en incident finns dock inte klart uttryckt. Detta gör att det finns risk för att användarstöden inte rapporterar in incidenter på ett enhetligt sätt eller att samtliga incidenter inte rapporteras in till helpdesk utan i stället åtgärdas direkt av användarstöden. Ansvaret för hantering av incidenter finns endast muntligt uttryckt och har inte formaliserats.

Enligt informationssäkerhetspolicy och instruktion för informationssäkerhet vid Migrationsverket ska loggar granskas regelbundet. Driftstörningar, intrång, kriminella handlingar och annat av betydelse för verksamheten ska följas upp. I intervjuer framkom dock att Migrationsverket inte har tillgång till några tekniska hjälpmedel som på ett systematiskt sätt kan söka av de loggningar som sker i systemen. Den granskning av loggar som sker är dessutom i hög grad inte proaktiv utan sker snarare efter det att verket fått indikationer på problem från andra källor. Det sker heller ingen dokumentation av den loggranskning som utförts med undantag för de ärenden som tagits upp i personalansvarsnämnden, vilket gör det svårt att se omfattningen av genomförda granskningar inom verket. Dessutom finns det vissa system där loggning inte kan utföras, vilket begränsar möjligheten till uppföljning.

Enligt instruktion om informationssäkerhet vid Migrationsverket ska huvudkontorets IT-funktion ansvara för verkets gemensamma IT-verksamhet. I detta ingår att kontrollera, åtgärda och följa upp det arbete som utförs av externa leverantörer. Enligt intervjuer har någon formell uppföljning av driftleverantörens arbete inte gjorts, dock hålls månatliga driftmöten samt kvartalsvisa teknikmöten.

Migrationsverket har vidare inte kunnat presentera någon kontinuitetsplan/avbrottsplan trots att verket i instruktion om informationssäkerhet vid Migrationsverket beslutat att en avbrottsplan ska upprättas och uppdateras fortlöpande för verksamhet som är beroende av IT-stöd. I intervjuerna har framkommit att många verksamheter och system har höga krav på tillgänglighet för att verksamheten ska kunna fungera. Vad gäller kontinuitetsplan/avbrottsplan för driften hänvisas i några intervjuer till att driften av IT-verksamheten är utlagd på underleverantör samt att företaget som ansvarar för verkets IT-drift ansvarar för att ha en sådan plan upprättad. Som tidigare nämnts har ingen formell uppföljning av driftleverantörens arbete skett. Migrationsverket har inte verifierat att underleverantören har upprättat någon avbrottsplan.

Av instruktion om informationssäkerhet vid Migrationsverket framgår att behörigheterna ska sättas efter individens behov i arbetet. När en användares behov upphör eller ändras ska behörigheten anpassas. Vid intervjuerna framkom dock att det i dag inte finns någon formaliserad uppföljning av att personalen har behörigheter anpassade efter sina arbetsområden och att det är tveksamt om dessa anpassningar av personalens behörigheter utförs i någon högre grad vid verket. Vidare har flera intervjuade sett svagheter i den rutin som finns för tilldelning av behörigheter. Flera svagheter i behörighetsrutinen har också identifierats vid en, av Riksrevisionen, tidigare genomförd behörighetsgranskning. Migrationsverket har meddelat Riksrevisionen att vissa åtgärder nu har vidtagits för att komma till rätta med dessa brister.

I intervjuerna har framkommit att säkerhetsfrågorna hittills inte tagits upp tillräckligt tidigt i systemutvecklingen. Systemsäkerhetsanalyser för respektive utvecklingsprojekt har inte utförts. I och med utvecklingen av EU-systemet VIS har Migrationsverket använt sig av ett metodstöd för utvecklingen, och en säkerhetsanalys har upprättats för detta system.

En granskning av dokumenten visar att de delar som behandlar distansarbete och användning av e-post är väldigt övergripande och inte tar upp alla aspekter som kan anses vara relevanta. Rörande användning av e-post behandlar policyn i stort sett endast vilka informationsklasser som får skickas med olika krypteringssystem. De informationsklasser som anges här är dessutom inte beslutade och används heller inte i praktiken. I intervjuer har dessutom risken för att inkommande e-postmeddelanden inte diarieförs tagits upp.

5.3 Bedömning

Riksrevisionens bedömning är att LIS-standardens kontrollfunktioner endast delvis finns på plats. Granskningen visar att ett flertal kontrollfunktioner saknas eller har brister i sin utformning och att verkets ledningssystem inte i tillräcklig utsträckning fungerar utifrån best practice.

Migrationsverket har inte utvecklat några uttryckliga mål till vilka informationssäkerhetsriskerna kan kopplas för de enskilda verksamhetsområdena, vilket är en brist enligt Riksrevisionens bedömning. Även kontinuitetsplaner för verksamheten saknas. Detta leder enligt Riksrevisionens bedömning till att ledningen i sin uppföljning av brister inom informationssäkerhetsområdet inte kan ställa dessa brister mot verksamhetens behov och krav inom området. Ledningen saknar enligt Riksrevisionens bedömning fastställda rutiner för att informera sig om verkets säkerhetsläge. Ledningen saknar

därigenom överblick över de behov som respektive verksamhetsområde har för sin informationssäkerhet.

Riksrevisionen kan vidare konstatera att Migrationsverket inte har upprättat beslutade och finansierade åtgärdsplaner för de brister som framkommit i tidigare utförda säkerhetsgenomgångar. Enligt Riksrevisionens bedömning försämrar detta ledningens förutsättningar för införandet av viktiga kontrollfunktioner avseende informationssäkerheten.

Migrationsverket har vidare brister i behörighetsrutinerna och i uppföljningen av att behörigheterna är anpassade till personalens arbetsuppgifter. Detta kan enligt Riksrevisionens bedömning leda till en ökad risk för att obehöriga får tillgång till känslig information.

Migrationsverkets granskning av loggar är i hög grad inte proaktiv, vilket enligt Riksrevisionens bedömning ger sämre förutsättningar att upptäcka eventuellt missbruk av information eller felaktigheter i systemen i ett tidigt skede. Att loggranskning faktiskt sker är dessutom svårt att verifiera eftersom det inte finns någon dokumentation av utförda granskningar.

Den del i instruktion om informationssäkerhet vid Migrationsverket som avser e-post och kommunikation är inte heltäckande. Det saknas t.ex. etiska regler beträffande vad som får skrivas i e-post, vilket enligt Riksrevisionens bedömning är ett viktigt område att ta hänsyn till för Migrationsverket.

Det faktum att kontrollfunktioner som beslutats av verksledningen saknas eller är bristfälliga gör att Riksrevisionen finner brister i ansvarstagande och i uppföljningen av att väsentliga kontrollfunktioner faktiskt införts. Ledningens bristande möjlighet till överblick tillsammans med bristande uppföljning av kontrollfunktionerna leder till en ökad risk i form av otillräckligt skydd för incidenter och otillräckliga möjligheter att hantera konsekvenser av dessa. Dessa brister i ledningssystemet för informationssäkerhet kan påverka informationssäkerheten 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 ledningssystemet. 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[22]. 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

Migrationsverkets styrande dokument för informationssäkerhetsarbete är tillgängliga via intranätet, där det även finns vissa anvisningar avseende incidentrapportering.

Enligt Migrationsverkets styrdokument är respektive verksamhetschef ansvarig för att personalen får säkerhetsutbildning som är anpassad för de aktuella arbetsuppgifterna. Detta antas gälla även inom delområdet informationssäkerhet, dvs. cheferna ska ge personalen förutsättningar att inhämta kunskap om informationssäkerhetsfrågor. Varje medarbetare har ett ansvar att ta del av anvisningar och regler för säkerhet samt att följa de regler som anvisas av ledningen. Säkerhetsenheten ansvarar för att ta fram handböcker m.m. inom sitt ansvarsområde.

I informationssäkerhetspolicyn definieras vad som avses med informationssäkerhet; viktiga begrepp anges också. Vidare betonas vikten av att alla

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

anställda inom verket är medvetna om informationssäkerhetens betydelse och har kunskaper om vad som gäller för att bevara och utveckla en säker och stabil IT-miljö.

Enligt instruktion om informationssäkerhet vid Migrationsverket ska användare ha nödvändiga kunskaper om system och gällande säkerhetsrutiner innan tilldelning av behörighet sker. Jämfört med de krav som ställs i LIS-standarden noteras att reglering av informationssäkerhetsfrågor i anställningsavtal inte har införts vid Migrationsverket.

Flera verksamhetsområdeschefer utsågs i juni 2006 till systemägare. Dessa verksamhetsområdeschefer har dock inte genomgått utbildning i informationssäkerhet. En utbildningsinsats har genomförts på vissa enheter under våren och sommaren 2006, men någon **process** för samlad, obligatorisk utbildning i informationssäkerhetsfrågor för personal och chefer finns i dag inte vid Migrationsverket.

6.3 Bedömning

Migrationsverket saknar en systematisk process för utbildning i informationssäkerhetsfrågor för såväl verksamhetsansvariga chefer som för övrig personal. Vissa centrala dokument rörande informationssäkerhet finns dock tillgängliga via intranätet. Sammantaget bedömer Riksrevisionen att de brister som iakttagits medför att Migrationsverket inte har säkerställt att personal, ansvariga chefer och systemägare får tillräcklig information om risker och hot inom informationssäkerhetsområdet, samt hur dessa ska hanteras. Detta medför enligt Riksrevisionens bedömning att informationssäkerheten riskerar att påverkas negativt, då berörda personalkategorier inte ges förutsättningar att fullgöra det ansvar som delegerats till dem.

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.

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.m.),
  - 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

Det finns inga **dokumenterade** riktlinjer för införande och **vidareutveckling** av ledningssystemet vid Migrationsverket. Enligt informationssäkerhetspolicyn ska dock **regelbunden** uppföljning göras av riskanalyser, informationsinsatser och säkerhetsåtgärder. Verksamhetschefer i organisationen har ett särskilt ansvar för att införa och vidmakthålla det som fastställts i policyn, medan säkerhetsskyddschefen har ett särskilt ansvar för att följa upp informationssäkerheten samt kontrollera regelefterlevnaden. Säkerhetsskyddschefen ansvarar även för att informationssäkerhetspolicyn regelbundet uppdateras.

Som tidigare konstaterats har några risk- och sårbarhetsanalyser i den form som beslutats i verkets instruktion om informationssäkerhet inte kunnat presenteras för Riksrevisionen vid granskningen. Avsaknaden av såväl en heltäckande informationsklassificering som dokumenterad riskanalys, medför att det inte finns någon grund att basera en konkret åtgärdsplan på. Den uppföljning som sker från säkerhetsenhetens sida är inte formaliserad i någon typ av uppföljnings- eller kontrollplan. Utvärdering av informationssäkerheten görs med hjälp av SBA Check, men resultatet av dessa kontroller rapporteras inte till ledningen enligt någon fastställd ordning. Dock anges att ledningsgruppen, inför Riksrevisionens granskning, har fått en övergripande muntlig genomgång av SBA Check.

Förutom de genomgångar som görs med hjälp av SBA Check har även vissa säkerhetsgenomgångar gjorts av FRA. Migrationsverket har inte upprättat någon åtgärdsplan för att åtgärda de brister som påtalats vid dessa genomgångar.

IT-enheten ansvarar för kontroll och uppföljning av det arbete som externa leverantörer utför. Denna kontroll genomförs enligt intervjuerna inte på något formaliserat sätt, utan sker i samband med regelbundna avstämningsmöten. Därutöver har det vid några tillfällen genomförts olika typer av tillgänglighetskontroller. Någon särskild kontroll av den personal som leverantören tillhandahåller görs inte då verket anser att man har god kännedom om denna personal.

7.3 Bedömning

Enligt Riksrevisionens bedömning saknar Migrationsverket en väl utvecklad strategi för hur kvaliteten i verkets ledningssystem ska upprätthållas och vidareutvecklas.

En grundläggande brist i Migrationsverkets informationssäkerhetsarbete är avsaknaden av riskanalyser och åtgärdsplaner, samt avsaknaden av såväl klassificering som uppdaterad förteckning av informationstillgångar. Dessa

brister medför enligt Riksrevisionens bedömning att uppföljningen av informationssäkerheten i dagsläget inte kan organiseras på ett strukturerat och effektivt sätt.

Någon återkommande rapportering till verksledningen har inte förekommit. Åtgärdsplaner för att hantera iakttagna brister har inte upprättats. Någon övergripande och samlad uppföljning för att styrka att verkets ledningssystem fungerar som ett sammanhållet[23] system har inte gjorts.

Riksrevisionen bedömer utifrån detta att Migrationsverket saknar en fullständig bild av vilka tillgångar som ska skyddas, mot vilka risker skyddet ska fokuseras och om lämpliga säkerhetsåtgärder faktiskt införs och fungerar.

Sammantaget är Riksrevisionens bedömning att uppföljningen av verkets ledningssystem har brister i systematik och regelbundenhet, vilket medför att det saknas förutsättningar för att förebygga, upptäcka och åtgärda informationssäkerhetsincidenter på ett effektivt sätt.

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

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 Migrationsverkets ledning 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

Riksrevisionen har i granskningen valt att lägga tyngdpunkten på verksledningens styrning och kontroll för att säkerställa informationssäkerheten. Denna styrning och kontroll benämns samlat verkets ledningssystem för informationssäkerhet. Denna avgränsning innebär bl.a. att faktiskt uppnådd säkerhet i enskilda system inte granskats.

Granskningen av Migrationsverkets ledningssystem för informationssäkerhet visar att verket infört vissa av de delar av ledningssystemet som bör finnas enligt standarden SS-ISO/IEC 17799. Bland dessa finns behörighetskontrollsystem, fysiskt skydd för IT-systemen, säkerhetskopiering och vissa andra säkerhetsåtgärder av administrativ och teknisk natur. Verket har också beslutat om en organisation för arbetet med informationssäkerhet samt utarbetat policydokument och riktlinjer för informationssäkerheten.

Dock finns brister i genomförandet av den beslutade organisationen samt i efterlevnaden av regelverket. Som framgår av rapporten är stora delar av verkets ledningssystem för informationssäkerhet mindre väl utvecklade. Bristerna medför att Migrationsverkets ledningssystem för informationssäkerhet sammantaget inte utgör en fullt ut lämpligt utformad och fungerande helhet. Detta inverkar i sin tur negativt på Migrationsverkets förmåga att samla de erfarenheter som gör systematisk förvaltning[24] av verkets ledningssystem möjlig. Bristerna i ledningssystemet har en negativ påverkan på möjligheterna att uppnå och vidmakthålla den av verksledningen eftersträvade nivån på informationssäkerheten.

[24] Med förvaltning avses här det systematiska förbättringsarbete som syftar till att förbättra verkets ledningssystem för informationssäkerhet.

Granskningen har haft till syfte att besvara frågan om Migrationsverket, utifrån gängse normer, arbetar systematiskt med sin informationssäkerhet. Riksrevisionen bedömer sammantaget att Migrationsverket inte fullt ut arbetar systematiskt med sitt ledningssystem för informationssäkerhet.

Bedömningen baseras på tre huvudsakliga brister, som redan har beskrivits mer ingående i de tidigare kapitlen. Nedan sammanfattas beskrivningen av bristerna.

8.1.1 Bristande möjlighet att överblicka risker och skyddsvärda tillgångar

Migrationsverkets ledning saknar enligt Riksrevisionens bedömning tillräckliga verktyg för att skapa en rättvisande och överblickbar bild av informationssäkerhetsriskerna i verksamhetens skilda delar. Denna brist medför enligt Riksrevisionens bedömning bl.a. svårigheter för verksledningen att avgöra om beslutade säkerhetsåtgärder är i linje med interna mål och riktlinjer för informationssäkerhetsarbetet samt externa regelverk.

Det finns i dag ingen samlad riskanalys som kan utgöra grund för prioritering och effektivt införande av säkerhetsåtgärder på informationssäkerhetsområdet. Trots att Migrationsverket beslutat att analyser ska genomföras, har detta inte gjorts på vare sig lokal nivå eller gemensamt för verket. Systemägare och verksamhetsansvariga har heller inte fått utbildning i informationssäkerhetsfrågor som stöd i detta arbete.

Även en heltäckande informationsklassificering saknas, vilket bl.a. exemplifieras av att Migrationsverket inte klassificerar tillgångarna utifrån tillgänglighetskrav trots att det vid intervjuer framförts att delar av verksamheten har mycket höga krav på tillgänglighet till informationsresurserna. Någon aktuell samlad förteckning över verkets samtliga informationstillgångar har inte kunnat presenteras. Beträffande såväl förteckning över informationstillgångar som klassificering av dessa uppfattas det i organisationen som oklart vem som ska ansvara för dessa aktiviteter.

De ovan beskrivna bristerna beträffande övergripande riskanalys och förmåga till översikt medför enligt Riksrevisionens bedömning en risk att prioritering och införande av kontrollåtgärder inte bygger på en tillräckligt tillförlitlig grund för att ge eftersträvad informationssäkerhet.

8.1.2 Brister i ledningens kontrollfunktioner samt införda säkerhetsåtgärder

Migrationsverket har vissa beslutade styrdokument som berör informationssäkerhetsfrågor. I dessa dokument behandlas i allt väsentligt vilka kontrollfunktioner som ska finnas och vem som har ansvar för att de utförs. Riksrevisionen har dock iakttagit flera brister i utförandet av kontrollfunktioner-

na. Kontinuitetsplaner saknas, trots att de ska upprättas enligt det interna regelverket och trots att företrädare för Migrationsverket vid intervjuer framfört att delar av verksamheten har mycket höga tillgänglighetskrav på informationsresurserna.

Det finns ingen systematisk utbildningsprocess för att säkerställa att nyckelpersoner inom säkerhetsarbetet erhåller tillräcklig och återkommande utbildning inom området. Detta innebär sammantaget en risk för att organisationens olika delar inte uppfattar och genomför arbetet med informationssäkerhet på ett likartat sätt.

Vid tidigare granskning, som utförts av Riksrevisionen, har brister identifierats i behörighetskontrollsystemet samt i uppföljningen av att behörigheter är anpassade efter personalens arbetsuppgifter. Brister i behörighetskontrollsystemet kan leda till ökad risk att obehöriga får åtkomst till känslig information.

Migrationsverkets granskning av loggar sker inte i syfte att upptäcka brister, utan utförs i hög grad efter det att verket fått indikationer på problem från andra källor. Detta försämrar, enligt Riksrevisionens bedömning, ytterligare förutsättningarna för att på ett tidigt stadium upptäcka eventuellt missbruk av information. Att loggranskning faktiskt sker har dessutom inte kunnat verifieras eftersom det inte finns någon dokumentation av utförda granskningar.

De exempel som nämnts ovan inverkar enligt Riksrevisionens bedömning negativt på Migrationsverkets förmåga att säkerställa att kraven på tillgänglighet till informationstillgångarna uppfylls. Detta försvårar dessutom för verket att säkerställa att obehöriga inte får åtkomst till känslig information.

8.1.3 Brister i utbildning och uppföljning

En grundläggande brist i informationssäkerhetsarbetet är den avsaknad som konstaterats ovan av såväl klassificering och aktuell förteckning över informationstillgångar som av riskanalys och åtgärdsplaner. Dessa brister försämrar ledningens möjligheter att arbeta systematiskt med prioriteringar och uppföljning av informationssäkerhetsarbetet.

Uppföljningen av informationssäkerheten är i nuläget inte organiserad på ett tillfredsställande sätt. Flera beslutade åtgärder, såsom upprättandet av riskanalyser och kontinuitetsplaner, har inte genomförts. Det saknas även rutiner för regelbunden rapportering av informationssäkerhetsfrågor till ledningen. Detta gäller även rapportering av utfallet av utförda säkerhetsgenomgångar. För de brister som iakttagits i säkerhetsgenomgångarna har åtgärdsplaner avsedda att hantera de aktuella bristerna inte upprättats. Migrationsverket kan därför, enligt Riksrevisionens bedömning, inte ge en

samlad bild av om de befintliga säkerhetsåtgärderna tillsammans ger ett fullgott skydd för verkets informationstillgångar.

Sammantaget är Riksrevisionens bedömning att uppföljningen av Migrationsverkets informationssäkerhet brister i systematik och regelbundenhet. Detta medför ökad risk för att informationssäkerhetsincidenter inte kan förebyggas, upptäckas och åtgärdas på ett för verket kostnadseffektivt sätt.

8.2 Rekommendationer

Brister i Migrationsverkets förmåga att skydda sina informationstillgångar kan leda till skada för enskilda personer. Om inte personuppgifter hanteras korrekt kan detta leda till fel i handläggningen av asyl-, tillstånds- och medborgarskapsärenden, vilket i slutändan kan leda till att fel beslut fattas. Ett positivt beslut om asyl samt beslut om medborgarskap kan inte återkallas oavsett om beslutet har fattats på fel grunder. Brister i förmågan att skydda informationstillgångarna kan också äventyra allmänhetens förtroende för Migrationsverket.

Riksrevisionens bedömning är att ett sammanhållet och tydligt ledningssystem för informationssäkerhet är en förutsättning för att Migrationsverkets ledning ska kunna förvissa sig om att beslutade säkerhetsnivåer uppnås. Detta kräver bl.a. att ledningssystemet stärker ledningens möjligheter till överblick av risker, behovet av säkerhetsåtgärder och kostnaderna för säkerhetsarbetet. Då framgår också tydligare vilket utrymme som finns för prioriteringar mellan olika säkerhetsinvesteringar. Ledningssystemet bör omfatta hela Migrationsverket och vara integrerat med övriga ledningssystem. Den i granskningen använda LIS-standarden innehåller, enligt Riksrevisionens bedömning, de viktigaste kraven på ett sådant ledningssystem. Det är dock ledningens ansvar att bestämma hur ledningssystemet ska utformas.

Migrationsverkets ledning bör fortsätta att genomföra åtgärder för att komplettera och dokumentera sitt ledningssystem. Riksrevisionen vill särskilt framhålla betydelsen av att ta fram en väl underbyggd riskanalys som grund för införande av relevanta säkerhetsåtgärder samt prioriteringar av dessa åtgärder. De beslutade säkerhetsåtgärderna bör dokumenteras i en åtgärdsplan som sedan utgör grund för systematisk uppföljning av att åtgärderna utförs och fungerar på det sätt som ledningen avsett. Riksrevisionen ser detta som en del av ett rapporterings- eller informationssystem som medger att verksledningen regelbundet och på ett specificerat sätt får tillgång till information från ledningssystemets skilda delar. Såväl specificering från ledningens sida av önskad återrapportering som regelbundenhet i denna återrapportering saknas i dag.

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)

Säkerhetsskyddslagen (1996:627)

Tryckfrihetsförordning (1949:105)

Förordningar

Arkivförordning (1991:446)

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

Datainspektionens allmänna råd: *Säkerhet för personuppgifter* (december 1999)

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

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

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

Standarder

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

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
2006:24 Granskningen av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten

Beställning: publikationsservice@riksrevisionen.se