RIKSREVISIONEN

Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten

ISBN 91 7086 094 7
RiR 2006:26
Tryck: Riksdagstryckeriet, Stockholm 2006

Till regeringen
Miljö- och samhällsbyggnadsdepartementet

Datum 2006-11-29
Dnr 31-2006-0338

Granskning av Lantmäteriverkets interna styrning och kontroll av informationssäkerheten

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

Företrädare för Lantmäteriverket 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. Rapporten överlämnas samtidigt till Riksrevisionens styrelse.

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

Riksrevisor *Karin Lindell* har beslutat i detta ärende. Granskningen har genomförts av revisionsledare *Maria Östman* (föredragande), revisionsdirektör *Stefan Gollbo* och revisionsdirektör *Carin Rytoft Drange*l. Biträdande granskningsområdeschef *Rutger Banefelt* och revisionsdirektör *Björn Undall* har medverkat i den slutliga handläggningen.

Karin Lindell Maria Östman

För kännedom:
Lantmäteriverket

Innehåll

Sammanfattning

Nästan en tredjedel av alla offentliga organisationer har utsatts för någon form av allvarligt dataintrång eller virusangrepp. Angreppen blir alltmer avancerade och allvarligare. Samtidigt lägger myndigheterna ut alltmer av sin verksamhet på Internet i form av elektroniska tjänster. Myndigheterna behöver därför arbeta med att skydda sin information och IT-stödet för verksamheten. Det är ett arbete som är både svårt och ofta resurskrävande. Det är mot denna bakgrund som Riksrevisionen har ökat sina insatser för att granska informationssäkerheten inom staten.

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

Under åren 2005–2006 har Riksrevisionen granskat informationssäkerheten vid tio statliga myndigheter. Denna granskning fokuserar på hur Lantmäteriverket 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?

Lantmäteriet, som består av Lantmäteriverket och en lantmäterimyndighet i varje län, har till uppgift att verka för en ändamålsenlig fastighetsindelning och en effektiv försörjning av grundläggande geografisk

information och fastighetsinformation. I detta ingår att tillhandahålla informationen så att samhällets behov tillgodoses vad gäller aktualitet och kvalitet. Lantmäteriverket har ett nationellt samordningsansvar för produktion, samverkan, tillhandahållande och utveckling inom grundläggande geografisk information och fastighetsinformation.

Viktig information hos Lantmäteriverket finns i fastighetsregistret, geografiska databaser och ett geodetiskt referenssystem. Det kan få allvarliga konsekvenser i samhället om geografisk information och fastighetsinformation inte är tillgänglig eller innehåller fel. Exempelvis kan enskilda drabbas eftersom informationen i fastighetsregistret ligger till grund för bankers och kreditinstituts långivning.

Har Lantmäteriverket ett fungerande system för informationssäkerhet?

Vid Lantmäteriverket finns flera fungerande delar av ett ledningssystem för informationssäkerhet. Vissa delar av ledningssystemet är dock inte tillräckligt väl utvecklade. Granskningen visar att ledningens informationssäkerhetsarbete har tre huvudsakliga brister: ansvarsfördelning är oklar, riskanalysarbetet har inte fullföljts och uppföljningen är inte systematisk. Det saknas t.ex. en tydligt utpekad ansvarig för uppföljning av att beslutade säkerhetsåtgärder införts. Lantmäteriverket har dock under 2006 påbörjat ett arbete som bl.a. syftar till en bättre riskanalys.

Bristerna innebär bl.a. att Lantmäteriverkets ledning inte har tillräckligt stöd eller tillräckliga hjälpmedel för att skapa överblick över, leda och följa upp informationssäkerheten. Bristerna medför att det finns en risk för att informationssäkerheten inte ligger på den nivå som är ledningens avsikt.

Sammantaget innebär bristerna att Lantmäteriverket inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

Riksrevisionens rekommendationer

Riksrevisionen bedömer att ett sammanhållet och tydligt ledningssystem för informationssäkerhet är en förutsättning för att Lantmäteriverkets ledning ska kunna förvissa sig om att beslutade säkerhetsnivåer kommer till stånd och bibehålls i hela myndigheten. Den i granskningen använda LIS-standarden innehåller enligt Riksrevisionens bedömning de viktigaste kraven på ett sådant ledningssystem. De delar av ledningssystemet som Lantmäteriverket särskilt bör utveckla är att:

- tydligare utforma och beskriva hur ledningssystemet ska fungera för att stärka ledningens möjligheter till överblick, prioritering och uppföljning.

- precisera och etablera en tydlig ansvarsfördelning.
- besluta hur riskanalysarbetet och en samlad planering av säkerhetsarbetet ska bedrivas.
- besluta om hur uppföljning av arbetet med informationssäkerhet ska bedrivas. Lantmäteriet bör även införa en systematisk uppföljning av IT-incidenter.
- fullfölja den påbörjade genomgången av system, systemägare och behov av reservdriftsrutiner.

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 Lantmäteriverkets ledning och styrning av arbetet med 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 användningsområden 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 och publicerats som granskningsrapporter: Sjöfartsverket, Statens Pensionsverk, Försäkringskassan, Lantmäteriverket, Migrationsverket och Arbetsmarknadsverket. Metoden har i vissa delar tillämpats i ytterligare fyra granskningar, som har rapporterats på annat sätt: Bolagsverket, Försvarsmakten, Post- och telestyrelsen samt Svenska Kraftnät

[2] enligt ISO 17799.

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

- 21 procent av statliga och kommunala myndigheter har någon gång varit med om IT-säkerhetsincidenter som medfört att information eller systemkomponenter blivit åtkomliga för obehörig att läsa, kopiera, ändra eller radera. Det kan alltså handla om dataintrång, hacking.
- 10 procent av statliga och kommunala myndigheter har varit med om IT-säkerhetsincidenter som inneburit att en angripare gjort en utförlig kartläggning av organisationens system, dvs. att obehörig letat efter sårbara punkter.
- 20 procent av statliga och kommunala myndigheter har varit med om IT-säkerhetsincidenter som medfört att system eller delar av system blivit 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 så kallade virus, maskar, trojaner m.m.

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

1.1.2 Syfte

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

Riksrevisionen har vidare valt att avgränsa granskningen till arbete 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 Lantmäteriet 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 således legat på myndighetsledningens styrning och kontroll för att säkerställa säkerheten hos eller skyddet av informationen i IT-systemen och andra informationstillgångar, såsom systemdokumentation, programkod och programlicenser. Denna styrning och kontroll benämns samlat myndighetens ledningssystem för informationssäkerhet. 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 vårt val av ledningssystem för informationssäkerhet som fokus för denna granskning.

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

1.2 Bedömningskriterier

I bedömningen av Lantmäteriverkets 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) innehåller riktlinjer som enligt standarden ”bör betraktas som ett underlag för att utveckla organisationsspecifika riktlinjer. Allt som nämns i LIS-standarden är kanske inte tillämpligt. Ytterligare åtgärder, som inte anges i denna standard, kan också

[5] Däremot har Riksrevisionen tagit del av dokument 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.

vara nödvändiga."[7]. Samtidigt utgör standarden "en gemensam grund för i princip alla organisationer"[8] [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 visats sig vara stabila. Standarden har efter tio år nu uppdaterats beträffande sin disposition men den är innehållsligt intakt.

1.2.1 Översikt över lagar och förordningar som berör informationssäkerhet

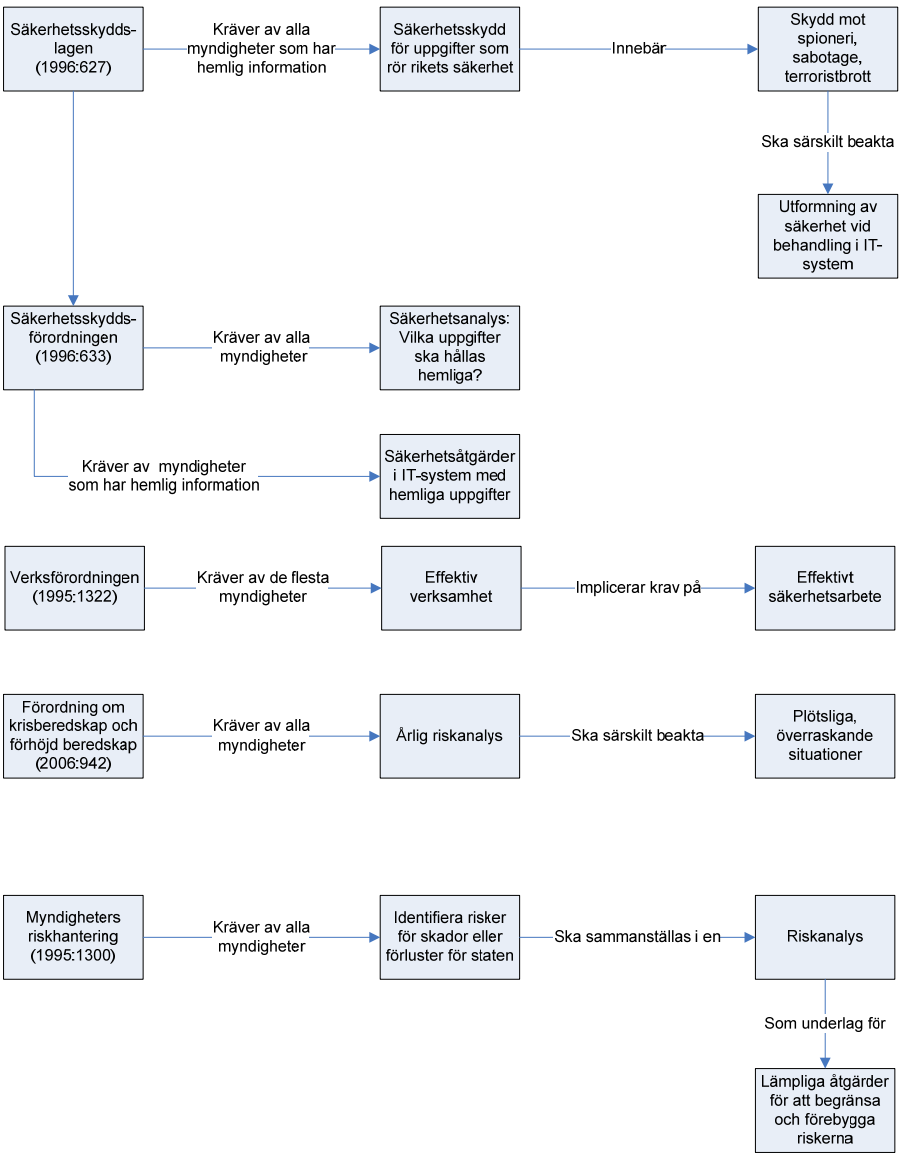
Lagar och förordningar som berör informationssäkerhetsområdet beskrivs i figuren nedan. De behandlar myndigheters riskhantering (förordning [1995:1300] om myndigheters riskhantering), åtgärder för fredstida krishantering (förordning [2006:942] om krisberedskap och höjd beredskap[10]) samt skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet (säkerhetsskyddslagen [1996:627]).

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

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

[9] 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.

[10] Tidigare förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap som upphävdes 2006-09-01.



Figur 1. Översikt över reglering av informationssäkerhet

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

- kravet att årligen analysera om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Särskilt ska beaktas situationer som uppstår hastigt, oväntat och utan förvarning eller situationer där det finns ett hot eller en risk att ett sådant läge kan komma att uppstå samt situationer som kräver brådskande beslut och samverkan med andra aktörer. Myndigheterna ska vidare särskilt beakta att de mest nödvändiga funktionerna kan upprätthållas i samhällsviktig verksamhet, och att förmågan att hantera mycket allvarliga situationer inom myndighetens ansvarsområde upprätthålls (9 § förordningen 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 spioneri, terroristbrott m.m. som kan hota rikets säkerhet (6 § 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 i den hemliga informationen. Förordningen 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, *skyddsvärd information* skyddas. Det innebär ett vidgat åtagande eftersom skyddsvärdet inte relateras till enbart rikets säkerhet eller till statsfinansiella förluster utan kan avse exempelvis enskilds

integritet och hälsa eller hemliga förhållanden i företag. Det som enligt regelverket ska göras av alla myndigheter – riskanalys, risk- och sårbarhetsanalys samt säkerhetsanalys – inryms samtidigt i standardens krav på främst ledningssystemets riskanalysprocess respektive den del av riskanalysen som avser säkerhetsklassificering av informationen.

Riksrevisionens slutsats är att LIS-standarden ligger i linje med regelverket. Skillnaderna är att regelverket täcker en mindre del av myndigheternas säkerhetsarbete (främst riskanalysen) och en mindre del av de statliga informationstillgångarna samt att regelverket är mindre preciserat med undantag för säkerhetsarbetet som gäller den hemliga informationen. LIS-standarden kan på så sätt sägas precisera kraven på myndigheternas arbete inom informationssäkerhetsområdet, men täcker även områden som inte direkt reglerats i lagar och förordningar.

Det ska tilläggas att det enligt Riksrevisionens bedömning även följer av 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[11]. 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.

[11] Committee of Sponsoring Organizations of the Treadway Commission (COSO) har beskrivit den interna styrningens och kontrollens olika beståndsdelar och deras samband i den s.k. COSO-modellen. Kapitlen 3-7 i Riksrevisionens rapport anknyter till dessa beståndsdelar.

1.3 Metoder och tillvägagångssätt i granskningen

Granskningen har genomförts på följande sätt:

- Lantmäteriverket valdes ut för granskning på grund av sin omfattande hantering av samhällsviktig information. 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.
- Myndigheten har därefter fått besvara ett frågeformulär (dvs. en självutvärdering) 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 Lantmäteriverket blivit intervjuade[12] 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.

[12] Generaldirektör, säkerhetschef, IT-säkerhetschef, chefsjurist, internrevisor, IT-direktör, enhetschef för Marknad Informationsförsörjning, divisionschef Fastighetsbildning, divisionschef Informationsförsörjning, två förvaltningsledare Informationsförsörjning samt IT-chef för Fastighetsbildning.

Ett annat ord som används är ”tillräcklig”. Det är en bedömning som Riksrevisionen gör av hur långt Lantmäteriverket kommit i förhållande till Riksrevisionens tolkning[13] 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 Lantmäteriverket 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.

[13] 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 Lantmäteriverket och informationssäkerheten

2.1 Lantmäteriverkets verksamhet

Med Lantmäteriet avses Lantmäteriverket och de 21 statliga länsvisa lantmäterimyndigheterna. Lantmäteriverket är chefsmyndighet för lantmäterimyndigheterna i länen.

Enligt instruktion (1995:1418) och regleringsbrev är Lantmäteriverkets uppgift att svara för en effektiv och långsiktigt hållbar användning av fastigheter, mark och vatten. Detta ska ske genom[14]

- en ändamålsenlig fastighetsindelning
- en effektiv försörjning med grundläggande landskaps- och fastighetsinformation.

Lantmäteriverket har ett nationellt samordningsansvar för produktion, samverkan, tillhandahållande och utveckling inom området grundläggande geografisk information och fastighetsinformation. Lantmäteriverket svarar även för samordning och stöd vid genomförande av EG-direktiv inom verksamhetsområdet och ska i övrigt bevaka Sveriges intresse i det internationella arbetet inom verksamhetsområdet.

Inom Lantmäteriverket finns ett geodataråd som är rådgivande i frågor som rör verkets samordnande roll inom området geografisk information och fastighetsinformation (geodataområdet).

Det finns en överenskommelse mellan ett antal myndigheter om myndighetssamverkan vad gäller risk- och krishantering inom området geografisk information. Överenskommelsen innebär att Lantmäteriverket i samverkan med Sveriges meteorologiska och hydrologiska institut, Sjöfartsverket, Statens geotekniska institut, Sveriges geologiska undersökning, Vägverket, Räddningsverket, Statens strålskyddsinstitut och Krisberedskapsmyndigheten ska bidra till att tillgodose samhällets behov av samordnad och samverkande geografisk information i fredstida kriser, vid höjd beredskap och i krig.

I Lantmäteriverkets uppgifter ingår att tillhandahålla informationen på ett sätt som tillgodoser samhällets behov vad gäller bl.a. aktualitet och

[14] Informationen är hämtad från Lantmäteriverkets Risk- och sårbarhetsanalys 2005, årsredovisningen 2005 samt förordningen (1995:1418) med instruktion för det statliga lantmäteriet.

kvalitet samt att ansvara för de geodetiska rikssystemen och stöd för mätning som innefattar satellitbaserad lägesbestämning och navigering, GPS.

Till kärnverksamheten hör de delar som är av betydelse för att uppfylla uppdraget enligt ovan: insamling, ajourhållning och tillhandahållande av grunddata. Grunddata delas in i fastighetsinformation och geografisk information.

Fastighetsinformationen om landets alla fastigheter finns samlad i fastighetsregistret som består av fem delar: allmän del, inskrivningsdel, adressdel, byggnadsdel och taxeringsuppgiftsdel. I fastighetsinformationen ingår också en registerkarta som redovisar fastighetsindelningen, officialrätter samt planer och markreglerande bestämmelser. Fastighetsindelningen ligger till grund för äganderätt, kreditgivning, fastighetsbeskattning, folkbokföring m.m. I registren finns uppgifter om fastigheter och samfälligheter, planer och bestämmelser, ägare, köp- och säljinformation, inteckningar, rättigheter, adresser och andra lägesuppgifter, mark- och taxeringsvärden.

Med geografisk information, i vidare mening, avses lägesbestämd information om förhållanden på eller under markytan, sjö- eller havsbotten. Den består bland annat av geografiska databaser, kartor, flygbilder och ett geodetiskt referenssystem.

Lantmäteriet omsätter ca 1,5 miljarder kronor per år och finansieras främst genom avgifter men även genom anslag. Uppdragsgivarna finns i såväl stat och kommun som det privata näringslivet och bland enskilda medborgare. Naturvårdsverket, Försvarsmakten, Handelsbanken, Vägverket och Banverket är Lantmäteriets största kunder. Övriga kundgrupper finns framför allt inom fastighetsvärdering, bank- och kreditväsende. Andra användare av geografisk information och fastighetsinformation finns inom räddningstjänst, polis, ambulans, sjukvårdsinrättningar, myndigheter såsom Statistiska centralbyrån, Skatteverket m.fl.

Lantmäteriet är organiserat i tre divisioner med ansvar för olika verksamhetsområden: Fastighetsbildning som har ansvar för fastighetsindelningen, Informationsförsörjning som bygger upp och tillhandahåller geografisk information och fastighetsinformation och Metria som bedriver uppdragsverksamhet. Lantmäteriet har sammanlagt något över 2 000 medarbetare fördelade på omkring 100 orter. Huvudkontoret ligger i Gävle.

De förvaltningsrättsliga föreskrifter som reglerar Lantmäteriets verksamhet är förutom regleringsbrevet och instruktionen (1995:1418) i huvudsak:

- Lagen (2000:224) om fastighetsregister
- Förordningen (2000:308) om fastighetsregister
- Lagen (1993:1742) om skydd för landskapsinformation
- Förordningen (1993:1745) om skydd för landskapsinformation

- Förvaltningslagen (1986:223)
- Sekretesslagen (1980:100)
- Personuppgiftslag (1998:204)
- Lagen (1992:1528) om offentlig upphandling
- Arkivlagen (1990:782)

Därutöver finns föreskrifter (LMVFS) som Lantmäteriverket utfärdar.

2.2 Informationstillgångarna och Lantmäteriverkets bedömning av säkerheten för dessa

Lantmäteriverkets bedömning är att vid utebliven tillgång till geografisk information och fastighetsinformation kan krissituationer uppstå i verksamheten hos stora användare i samhället.

Lantmäteriverket är sedan april 2003 (förnyat i april 2006) certifierat enligt ISO 14001 och har i samband med det byggt sitt ledningssystem enligt ISO 9001.

Inslaget av IT-stöd i Lantmäteriets processer är betydande, och verksamheten är mycket starkt IT-beroende. Lantmäteriet har en mängd system, både egenutvecklade och standardprogramvaror.

Viktiga IT-system hos Lantmäteriet är bl.a.:

- Fastighetsregistret, inkluderande registerkartan, som består av både av stordator- och Unix/Windows-miljöer.
- Trossen, ett handläggningssystem för fastighetsbildningen, som består av både Unix- och Windows-miljöer.
- System för grundläggande geografisk information, mestadels i Unix-miljö.
- Arken, ett digitalt förrättningsarkiv, mestadels i Unix-miljö.

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

Enligt Lantmäteriverkets svar på Riksrevisionens enkät[15] betraktas informationssäkerhet som en viktig ledningsfråga som myndigheten under en tid inte haft möjlighet att i önskvärd utsträckning uppmärksamma.

Ett flertal faktorer i verksamheten påverkar myndighetens bedömning av informationssäkerhetens betydelse. Lantmäteriverket framhåller i sitt svar på enkäten följande faktorer som särskilt betydelsefulla för utformningen av

[15] Riksrevisionens enkät avseende IT-säkerhet. Svar erhållet 2006-05-12.

arbetet med informationssäkerhet/IT-säkerhet: omfattningen av IT-beroendet, omfattningen av e-tjänster och exponeringen på Internet, vikten av kontinuitet, volymen förvaltade anläggningstillgångar samt storleken på penningströmmar i verksamheten.

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

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 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 eller 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 enskilda medarbetaren.

3.2 Iakttagelser

LIS-standarden anger att ett uttryck för ledningens **engagemang** för informationssäkerhet är att ledningen preciserar ett ansvar och aktiviteter för att få nödvändig överblick över informationstillgångarna så att det blir möjligt att göra en riktig prioritering av skydd och skyddsåtgärder. Prioriteringen ska enligt standarden baseras på en riskanalys.

Lantmäteriverkets GD beslutade under 1999 att informationssäkerhetsarbetet inklusive IT-säkerhet vid Lantmäteriverket ska bedrivas enligt Lantmäteriverkets *Riktlinjer för informationssäkerhet*[16]. Samtidigt beslutades att ansvaret för IT-system ska följa anvisningarna i *PM, Systemägare. Definitioner, ansvar, roller. Relation till IT-infrastrukturen*[17] där även rollen förvaltningsansvarig preciseras. Lantmäteriverkets *Riktlinjer för informationssäkerhet* motsvarar en **informationssäkerhetspolicy**.

Av riktlinjerna framgår tydligt att GD är ytterst ansvarig för informationssäkerheten. Här framgår vidare att ”Ansvaret för att vidta de säkerhetsåtgärder som krävs i olika system ligger inom respektive förvaltningsorganisation för systemen och tillhörande information”, vilket Lantmäteriverket kallar förvaltningsansvaret.

Riktlinjerna beskriver organisationen av informationssäkerhetsarbetet inom Lantmäteriverket. Här preciseras att GD fastställer riktlinjer och föreskrifter och att GD:s uppföljning i första hand sker genom rapportering från säkerhetschefen alternativt biträdande säkerhetschefer. Ansvaret för det faktiska säkerhetsarbetet ligger i förvaltnings- och linjeorganisationerna och härtill är kopplat befogenheter att välja de skyddsåtgärder som krävs för att uppnå målen för informationssäkerhetsarbetet. Häri ingår att bedöma säkerhetsnivån och anpassa den till övrig verksamhet. Vidare anges att varje systemägare har ansvaret för säkerheten i de egna systemen.

Under 2005 gjordes en omorganisering av ledningen inom Lantmäteriverket, och den nuvarande organisationen framgår av Lantmäteriverkets arbetsordning och beslut om förtydligande och effektivisering av Lantmäteriets lednings- och stödfunktioner[18]. En stab till generaldirektören (GD-stab) bildades med ansvar för koncernövergripande frågor, däribland IT-säkerhetsfrågor. Liksom tidigare finns därutöver en säkerhetschef som är placerad direkt under GD och som föredrar säkerhetsskyddsfrågor direkt inför GD. Inom GD-stab finns en person med ansvar för IT-säkerhet. Det finns däremot inget formellt beslut kring den IT-säkerhetsansvariges roll, mandat och ansvar.

I *Riktlinjer för informationssäkerhet* anges att säkerhetschefen har det av GD delegerade ansvaret för informationssäkerhet och att det som stöd till denne och systemägarna finns en funktion för informationssäkerhet. I dag består denna funktion av IT-säkerhetsansvarig och till viss del en beredningsgrupp för IT-frågor (vilket inte är helt i överensstämmelse med riktlinjerna). Om frågor tas upp i beredningsgruppen som avser beslut i frågor om informationssäkerhet ska samråd ske med säkerhetschefen.

---

[16] Riktlinjer för informationssäkerhet, Lantmäteriverket 1999-03-04.

[17] PM, Systemägare. Definitioner, ansvar, roller. Relation till IT-infrastrukturen, Lantmäteriverket 1999-02-15.

[18] Lantmäteriverkets interna regelsamling, LMVIR 2005:1 samt beslut A§486, daterad 2005-06-21.

Som framgår av riktlinjerna har det operativa ansvaret för säkerheten delegerats till systemägarna. Varje systemägare ska t.ex. ”bedöma i vilken omfattning och på vilket sätt skyddsåtgärderna skall tillämpas”[19]. Systemägaren har därmed en viktig roll för informationssäkerheten inom Lantmäteriet. I flera intervjuer har framgått att det är divisionschefen som formellt är systemägare om systemägarskapet inte delegerats. Samtidigt har det framkommit att det inom Lantmäteriet likväl är oklart vilka som är systemägare. Under intervjuerna har därtill framkommit att ansvaret för informationssäkerheten i praktiken ligger på förvaltningsansvariga. Riksrevisionen har även noterat att det inom Lantmäteriverket finns olika förvaltningsmodeller och att begrepp som systemägare och förvaltningsansvarig inte används konsekvent i hela organisationen. Exempelvis används systemägarbegreppet inte inom informationsförsörjningsdivisionens förvaltningsmodell.

Det finns brister avseende ledningens systematiska uppföljning av gjorda delegationer inom informationssäkerhet, t.ex. av systemägarnas arbete. Detta påverkar ledningens **förtrogenhet** med informationssäkerhetsarbetet. Den uppföljning Riksrevisionen noterat att Lantmäteriverket gör är rapportering av allvarliga incidenter, dvs. hanteringen av uppkomna brister i säkerheten. Hur ledningen ska följa upp gjorda delegationer framgår inte av granskade dokument. Uppföljning är också ett viktigt uttryck för ledningens **engagemang**. Mer om uppföljning finns i kapitel 7.

Av intervjuerna har framkommit att det finns ett engagemang och en medvetenhet inom Lantmäteriet avseende informationssäkerhetsfrågor. Det har även framförts att Lantmäteriverket strävar mot LIS-standarden. Lantmäteriverkets ledning har uppmärksammat att det finns problem, bl.a. att systemägarbegreppet inte varit tydligt, och i styrkorten till 2006 års verksamhetsplan har ledningen gett organisationen i uppdrag att identifiera de IT-system som finns och utse systemägare till alla system. Till det andra kvartalet 2006 har en första kartläggning genomförts. Vid IT-säkerhetsansvarigs genomgång av rapporteringen från divisionerna framkommer att utpekade systemägare ännu inte är införstådda med sitt ansvar.

I Lantmäteriverkets budget går det inte att särskilja arbetet med informationssäkerhet.

3.3 Bedömning

Systemägarna har hos Lantmäteriverket en nyckelroll i arbetet med informationssäkerheten. Det finns dock flera otydligheter i systemägar-

[19] Kapitel 5.1, Riktlinjer för informationssäkerhet.

begreppet hos Lantmäteriverket, och ledningen har inte infört någon systematisk återrapportering och uppföljning av det arbete som utförs av systemägarna. Detta försvårar, enligt Riksrevisionens bedömning, ledningens möjligheter att få en samlad bild av hur informationssäkerhetsarbetet i praktiken utförs i myndighetens olika delar.

Oklarheter finns också avseende IT-säkerhetsansvarigs uppgift och mandat, t.ex. ansvar för uppföljningsaktiviteter. Den IT-säkerhetsansvarige har en viktig funktion för ledningens arbete med informationssäkerhet.

De oklarheter som finns i rollerna och den bristande uppföljningen av informationssäkerhetsarbetet minskar ledningens möjlighet till överblick och styrning. Ledningen har därmed inte på ett tydligt sätt kunnat styra Lantmäteriverkets informationssäkerhetsarbete.

Riksrevisionen bedömer sammantaget att kontrollmiljön har brister, vilket kan leda till att informationssäkerheten påverkas 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 Lantmäteriverket har genomfört en adekvat riskanalys har Riksrevisionen använt följande sex kriterier.

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

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

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

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

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

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

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

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

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

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

4.2 Iakttagelser

Arbetet med riskanalyser är **organiserat** så att säkerhetschefen är ansvarig för riskanalyser enligt förordningen[23] (2002:472) om åtgärder för framtida krishantering och höjd beredskap. Att utföra riskanalyser för respektive system är delegerat till systemägarna [24].

Lantmäteriverket genomför riskanalyser enligt förordningen[23] (2002:472) om åtgärder för framtida krishantering och höjd beredskap. Risk- och sårbarhetsanalysen 2003 omfattade dels processer för kärnverksamheten, dels processer för verksamhet som är baserad på avtal och som kan anses viktiga för hur samhället kan nyttja geografisk information och fastighetsinformation för t.ex. krishantering.

I arbetet med 2003 års analys identifierades ett antal riskområden och utifrån dessa föreslogs tre åtgärder:

1) utreda samhällets behov av geografisk information och fastighetsinformation för krishantering och med detta resultat som grund utreda vilka processer i verksamheten för insamling, ajourhållning och leverans till användare som berörs [25]
2) utreda behov av alternativ driftplats, IT-miljö för produktion respektive säkerhetskopiering samt reservrutin[26]
3) utreda behovet av reservkraft för hela Lantmäteriet.

Lantmäteriverket har arbetat vidare med dessa frågor i Risk- och sårbarhetsanalysen både 2004 och 2005, och utredningarna har även lett till att krav på inventering och dokumentation av system och processer för viktiga samhällssystem finns infört i verksamhetsplanen för 2006. Ett arbete har påbörjats för att förbättra reservdriften i Unix-miljön.

De genomförda risk- och sårbarhetsanalyserna är ett steg mot en klassificering av informationstillgångarna men det saknas fortfarande en överblickbar **förteckning** eller databas avseende de skyddsvärda informationstillgångarna. En förteckning bör även innehålla dokumentation,

---

[23] Denna förordning har upphävts 2006-09-01 och ersatts av förordning (2006:942) om krisberedskap och höjd beredskap.

[24] I enlighet med Riktlinjer för informationssäkerhet, Lantmäteriverket 1999-02-15.

[25] Utmynnade i Rapportsammanställning 2004 års studie Samhällets behov av geografisk information och fastighetsinformation för krishantering.

[26] Utmynnade i rapport Reservarbetsplats 2006-02-07.

programkod, licenser m.m. I verksamhetsplanen 2006 ingår uppdraget att i första steget identifiera samtliga IT-system samt att utse en systemägare för varje system. Nästa steg är att göra risk- och sårbarhetsanalyser för de viktigaste systemen för att systematiskt bedöma om det behövs reservrutiner och hur dessa ska utformas.

Lantmäteriverket har för närvarande inte planerat en sådan förteckning över informationstillgångarna som krävs för att göra en fullständig **informations- eller säkerhetsklassning** av tillgångarna. I Lantmäteriverkets *Riktlinjer för informationssäkerhet* [27] anges att informationen i olika system ska vara klassificerad samt att det ska finnas riktlinjer för informationsklassning. Detta har ännu inte genomförts.

Informationen som behandlas i Lantmäteriets system kan grovt delas in i tre kategorier: information som är hemlig av totalförsvarsanledning, övrig information som avser karta och fastighet samt annan information. Lantmäteriverket har till viss del en säkerhetsklassificering då den hemliga informationen behandlas med sekretess. Informationen som rör totalförsvaret hanteras genomgående i särskild ordning inom Lantmäteriverket, och säkerhetskontroller genomförs av de särskilda myndigheter som har detta som uppgift.

I Lantmäteriverkets *Riktlinjer för informationssäkerhet* [27] anges att det ska finnas risk- och sårbarhetsanalyser, avbrotts- och katastrofplaner samt uppföljning för enskilda system. Lantmäteriverkets ledning har dock ingen systematisk uppföljning eller förteckning av vilka analyser och planer som är upprättade för enskilda system. Riksrevisionen kan därmed inte bedöma i vilken utsträckning riktlinjerna följs.

Ansvaret för att utföra riskanalyser för de respektive systemen har delegerats till systemägaren[27]. Riskanalyser har utförts för vissa av systemen, ofta initierat av kommande förändringar. Det finns en föreslagen **metod** för riskanalyserna (TRAQ[28]) men systemägaren har rätt att välja annan metod.

I verksamhetsplanen 2006 anges att risk- och sårbarhetsanalyser ska göras för de viktigaste systemen. GD-stab kommer att koordinera analyserna och har valt att använda TRAQ för dessa analyser.

Riskanalyser bör omfatta **alla typer av risker**, dvs. bristande tillgänglighet, riktighet, sekretess och spårbarhet, som kan vara väsentliga i verksamheten. De riskanalyser för enskilda system som Riksrevisionen har tagit del av (Trossen[29] och anpassningar av Arc Cadastre[30]) har fokuserat på förändringar inom systemet, och delområdet sekretess har utelämnats. Analysen för

---

[27] Riktlinjer för informationssäkerhet, Lantmäteriverket 1999-02-15.

[28] TRAQ står för ”Threat & Risk Assessment Questionnaire” vilket är en, av Lantmäteriverket, inköpt metod för risk- och sårbarhetsanalys som myndigheten själv kan tillämpa.

[29] Riskanalys för Trossen 2004-03-24.

[30] Riskanalys av Arc Cadastre och Fbas 2006-03-06.

just dessa system omfattade, enligt Lantmäteriverket, ej sekretess eftersom de inte hanterar någon sekretessbelagd information.

Incidenter hanteras av förvaltningsansvarig på systemnivå och större **incidenter** rapporteras till IT-säkerhetschef som i sin tur rapporterar till GD. Det finns ingen systematisk dokumentation av incidenterna på central nivå, med konsekvensen att någon samlad bild av upptäckta säkerhetsproblem inte kan skapas. Riksrevisionen kan därför inte bedöma hur stor andel av uppkomna incidenter som rapporteras till IT-säkerhetschefen.

Det finns ingen uppföljningsbar **åtgärdsplan** på central nivå, som förtecknar beslutade säkerhetsåtgärder och som i sin tur baserats på en samlad riskanalys och incidentrapportering. Åtgärderna finns spridda i andra dokument, bl.a. systemförvaltningsplaner.

4.3 Bedömning

Lantmäteriverkets verksamhet är omfattande och komplex, och det gäller även myndighetens informationstillgångar. Det är därför en brist i Lantmäteriverkets arbete med informationssäkerhet att det inte finns någon förteckning eller databas som ger en överblick över informationstillgångarna. En sådan förteckningen skulle kunna användas för att visa de säkerhetskrav som gäller för varje enskild tillgång samt de säkerhetsåtgärder som vidtagits för att skydda dem. Avsaknaden av en förteckning påverkar möjligheterna till systematisk riskhantering negativt.

I *Riktlinjer för informationssäkerhet* anges de dokument avseende informationssäkerhet som ska upprättas för respektive system. Ansvaret för att ta fram dokumenten har delegerats till respektive systemägare utan någon central uppföljning. En central uppföljning av uppgifterna i *Riktlinjer för informationssäkerhet* skulle ha säkerställt en riskanalys mer i enlighet med LIS-standarden. Avsaknaden av en samlad riskanalys och en central åtgärdsplan försämrar ledningens förmåga till styrning.

Sammantaget bedömer Riksrevisionen att Lantmäteriverkets riskanalys har sådana brister att det innebär förhöjd risk för informationssäkerheten hos Lantmäteriverket.

5 Ledningens kontrollfunktioner och säkerhetsåtgärder

5.1 Bedömningskriterier

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

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

Ledningssystemet bör normalt ha följande **omfattning** när det gäller komponenter[31]:

- informationssäkerhetspolicy,
- process för incidentrapportering inklusive beslut om vilka incidenter som ska rapporteras till ledningen,
- åtgärdsplan för informationssäkerhet,
- kontinuitetsplan,
- utsedd person med övergripande och samordnande ansvar för myndighetens informationssäkerhet,
- internetpolicy,
- distansarbetspolicy,
- e-postpolicy,
- åtkomstpolicy[32],
- process för säkerhetskopiering av all verksamhetskritisk information,

[31] 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.

[32] Policy som reglerar åtkomst till informationstillgångar.

- process för styrning av utveckling och förändringar i IT-miljö, IT-system och bemanning,
- tekniska säkerhetsåtgärder (behörighetskontrollsystem, virusskydd, brandväggar m.m.),
- processer för att kontrollera efterlevnaden av det regelverk för att upprätthålla informationssäkerhet som bl.a. ovannämnda policykomponenter tillsammans bildar,
- en till all personal kommunicerad skriftlig beskrivning av roller[33] 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**[34] 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

Av enkäten till Lantmäteriverket framgår att Lantmäteriverket valt att utforma sitt ledningssystem för informationssäkerhet utifrån delar av OFFLIS (Statskontoret) och BITS (Krisberedskapsmyndigheten). Under intervjuerna har framkommit att Lantmäteriverkets ambition är att närma sig LIS-standarden.

Granskningen visar att Lantmäteriverket har delar av ett ledningssystem för informationssäkerhet med **beslutade och dokumenterade komponenter**. De delar av ett ledningssystem som införts vid Lantmäteriverket omfattar övergripande policydokument och riktlinjer, ansvarsfördelning och organisation av säkerhetsarbetet samt ett stort antal tekniska säkerhetsåtgärder. Det finns dock brister i vissa av dessa komponenter och andra saknas till stor del jämfört med **best practice.** Dessa brister beskrivs nedan.

Styrande interna dokument för informationssäkerheten är främst arbetsordningen som bl.a. reglerar säkerhetschefens och stabens ansvar för IT-säkerhet och *Riktlinjer för informationssäkerhet*[35] där principen att varje systemägare har det operativa ansvaret för säkerheten i de egna systemen

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

[34] 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.

[35] Riktlinjer för informationssäkerhet, Lantmäteriverket 1999-02-15.

etableras inom Lantmäteriet. Informationssäkerhetsarbetet inom Lantmäteriverket bedrivs främst inom ramen för respektive system/förvaltningsobjekt. Arbetet med förvaltningsobjekten leds i praktiken av en förvaltningsledare i enlighet med av förvaltningsansvarig beslutad förvaltningsplan. Förvaltningsansvarig är på så sätt systemägarens företrädare för det praktiska utförandet. Dessa begrepp och arbetssätt skiljer sig dock åt mellan Lantmäteriverkets tre divisioner. Det finns också oklarheter i begrepp och roller, vilket framgår av kapitel 3.

Det finns en annan otydlighet i gränsdragningen mellan övergripande ansvariga – GD och säkerhetschef i relation till systemägarna. GD har det övergripande strategiska ansvaret medan systemägare, enligt *Riktlinjer för informationssäkerhet*, har befogenhet att välja de skyddsåtgärder som krävs. Detta innebär att systemägare/förvaltningsansvarig kan välja att inte införa kontroller som inte upplevs motiverade ur dennes perspektiv trots att de beslutats i policy eller riktlinje, vilket i så fall påverkar i vilken **omfattning** centrala policyer och riktlinjer verkligen är **införda** i organisationen.

Flera av de granskade dokumenten är inaktuella. De har äldre datum, innehåller förhållanden och beskrivningar som inte gäller längre inom Lantmäteriverket samt är i vissa delar inte färdigställda. Ett exempel på detta är portaldokumentet *Riktlinjer för informationssäkerhet* som är daterat och beslutat 1999.

Processen för incidentrapportering regleras i dokumentet *Processen för hantering av IT-incidenter* (2003-01-20). Av detta framgår inte att alla anställda är skyldiga att rapportera incidenter, det framgår inte heller att IT-säkerhetsansvarig ska få rapportering om alla incidenter. Det ställs inte heller några krav på att IT-säkerhetsansvarig ska göra någon sammanställning av inträffade och inrapporterade incidenter som ett underlag för riskanalys och bedömning av skyddsåtgärders införande och förändringsbehov. Detta ska i stället enligt samma dokument ske på systemnivå och göras av respektive förvaltningsansvarig. Dessa otydligheter bekräftas även av en rapport från internrevisionen[36], som avsåg de koncerngemensamma systemen, där det framgår att flera av de då intervjuade anser att ansvaret för incidenthantering inte är tydligt definierat.

De incidenter som upplevs som mer allvarliga har enligt uppgift rapporterats direkt till IT-säkerhetsansvarig som direkt informerat både säkerhetschef och GD, men det finns ingen fastställd rutin för eller regler om vilka incidenter som ska rapporteras till ledningen.

Det finns ingen samlad åtgärdsplanering avseende åtgärder för att förbättra och vidmakthålla informationssäkerhet inom Lantmäteriverket. Planering av åtgärder sker i stor utsträckning på lägre organisatorisk nivå –

[36] Incidenthantering koncerngemensamma system 2006-02-10, dnr 203-2005/1218.

division, enhet, funktion eller systemvis – vilket innebär att myndighetsledningen inte har kontroll/överblick över hur riskutsatt verksamheten är eller om den är olika riskutsatt i olika delar. Det saknas därmed ett underlag för prioritering över organisatoriska gränser i syfte att erhålla en gemensam säkerhetsnivå.

Kontinuitetsplaneringen vid Lantmäteriverket ser olika ut för olika systemdelar. Lantmäteriverket lever i olika driftmiljöer: en samlad stordatormiljö respektive distribuerade miljöer (främst Unix/Windows-miljöer). För de system som går i stordatormiljön finns i dag etablerade reservdriftsrutiner till stor del. För de distribuerade miljöerna är läget inte lika bra. I en intern rapport[37] från en utredning av Lantmäteriverkets behov av reservarbetsplats konstateras att systemägare inte är medvetna om sitt ansvar för säkerhetskopiering på annan plats och att det saknas reservrutiner för de flesta av Lantmäteriverkets system. Av bl.a. denna anledning har Lantmäteriverket i sin verksamhetsplanering för 2006 planerat att alla system ska identifieras och systemägare utses samt reservdriftsrutiner etableras med prioritering utifrån risk och väsentlighet. Vid intervjuer har även framkommit att medvetenheten är för låg om systemsamband och hur dessa påverkar förmågan till reservdrift.

Vid Lantmäteriverket finns en särskilt utsedd ansvarig för IT-säkerhet. Denna roll framgår av dokumentet *IT-säkerhetsprocessen*[38]. Enligt detta dokument ansvarar IT-säkerhetsansvarig för koordinering av arbetet med IT-säkerhet och att styrande dokument inom området utarbetas och beslutas. Som även framgår av kapitel 3 saknas dock formellt beslut avseende den IT-säkerhetsansvariges roll, mandat och ansvar. Omfattningen av tjänsten är ca 70 % av en heltid. IT-säkerhetsansvarig lyder linjemässigt direkt under IT-direktören och är även verksam i beredningsgruppen för IT-frågor (BIT), som är ett beslutsberedningsorgan för myndighetsgemensamma IT-frågor. Beslutande i BIT är IT-direktören och om en fråga avser IT-säkerhet samråder han med Lantmäteriverkets säkerhetschef.

Systemadministratörer avseende distribuerad Windows-miljö inom hela Lantmäteriet utgör en viktig länk i säkerhetskedjan. De är 50–75 personer både på huvudkontoret i Gävle och ute i landet. De är ansvariga för att upprätthålla en beslutad säkerhetsnivå i de lokala installationerna av bl.a. operativsystem, genom versionshantering och s.k. patchningar. Det finns dock inga specificerade krav på kompetens eller utbildning för dessa personer. Det finns inte heller någon systematisk uppföljning av deras arbete. Detta innebär en risk att genomförandet av installationer (patchningar m.m.) och inställningar genomförs på olika sätt i olika delar av Lantmäteriets gemensamma nätverk.

[37] Rapport reservarbetsplats, daterad 2006-02-07.
[38] IT-säkerhetsprocessen 2003-01-20.

Lantmäteriverket har ingen tydligt etablerad modell för säkerhetsklassificering av sin information. Behovet av att klassificera information avser framför allt gruppen karta och fastighet, där i princip all information är offentlig, men inte alla sammanställningar av samma information (säkerhetsklassificering tas även upp i kapitel 4).

En åtkomstpolicy saknas. Det finns ett antal behörighetskontroller och rutiner för behörighetshantering i de olika systemen, men det finns inget övergripande styrdokument på policynivå som reglerar principer, nivå eller inriktning för behörighetstilldelning och som är giltigt för hela Lantmäteriet.

Det finns inga tydliga riktlinjer eller moment i Lantmäteriverkets modell för systemutveckling för att säkerställa att informationssäkerhetskrav beaktas tidigt och tydligt vid verksamhets- och systemutveckling.

Ledningens åtgärder för att åstadkomma en strukturerad uppföljning och förvaltning av införda säkerhetsåtgärder har brister; dessa brister utvecklas i kapitel 7.

Utöver de redan nämnda styrdokumenten finns vid Lantmäteriverket ett antal policyer på plats som reglerar informationssäkerhet, t.ex. Internetpolicy, distansarbetspolicy och e-postpolicy.

5.3 Bedömning

Granskningen visar att Lantmäteriverket har många säkerhetsåtgärder på plats, men den visar också att flera kontroller inte finns på plats eller inte är tillräckligt väl utvecklade i jämförelse med best practice. Ledningen har infört flera av de delar som enligt LIS-standarden bör ingå i ledningssystemet. Bristerna som påpekats ovan påverkar dock den sammantagna ändamålsenligheten i ledningssystemet för informationssäkerhet vid Lantmäteriverket, och därmed bedömningen av om det ska anses vara ett väl fungerande system för ledningen.

Riksrevisionen bedömer att det finns brister främst avseende ledningens förmåga att åstadkomma ett helhetsperspektiv på informationssäkerheten för hela Lantmäteriet, t.ex. samlad åtgärdsplan, strukturerad incidentrapportering och kontinuitetsplanering.

Styrdokumenten är inte ändamålsenliga då de är inaktuella och inte speglar en tydlig och etablerad helhetssyn på ledningssystemet.

Ledningssystemets funktion är beroende av tydliga roll- och ansvarförhållanden; här finns också brister.

Sammantaget bedömer Riksrevisionen att konstaterade svagheter i styrning av säkerhetsåtgärderna och uppföljningen riskerar att informationssäkerheten påverkas negativt hos Lantmäteriverket.

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**[39]. 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

Det finns ingen systematisk **process** för utbildning av olika personalgrupper, inklusive chefer. Samtliga nyanställda genomgår en introduktionsutbildning som innehåller ett ca 20 minuter långt inslag om säkerhet. Under detta inslag nämns informationssäkerhet, och de nyanställda hänvisas till Lantmäteriverkets intranät och en folder om *IT- säkerhet i vardagen*. Någon systematisk information och utbildning ges inte därefter.

Lantmäteriverket informerar de anställda, via intranätet, om de interna regler som gäller informationssäkerhet. Här finns bl.a. riktlinjer för informationssäkerhet, säkerhetspolicy för system exponerade mot Internet och riktlinjer för basnivå för säkerheten i Ethel[40]. Dokumentationen är till viss del inaktuell.

En stor del av ansvaret vad gäller IT-systemen är delegerat till systemägare, förvaltningsledare och systemadministratörer. Det finns dock ingen

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

[40] Ethel är samlingsnamnet för Lantmäteriets gemensamma datanät och datakommunikation.

systematisk utbildning av dessa **berörda personalgrupper** i informationssäkerhet och om deras respektive ansvar.

Vissa utbildningsinsatser sker i samband med att en person får tillgång till ett visst IT-system, men detta är inte en del av en systematisk process för utbildning av olika personalgrupper, inklusive chefer.

Det finns ingen systematisk ansats att utbilda säkerhetspersonal för att nå en mer enhetlig uppfattning om vad arbetet med informationssäkerhet på olika nivåer i organisationen innebär och med vilka metoder det ska bedrivas.

6.3 Bedömning

Riksrevisionen bedömer att Lantmäteriverket inte hanterar behovet av fortlöpande information och utbildning inom informationssäkerhetsområdet på ett strukturerat sätt eller i övrigt på det sätt som LIS-standarden förutsätter. Ledningen har inte inrättat funktioner för att försäkra sig om att personalen får tillräckliga kunskaper om informationssäkerhet och följer de regler som finns internt inom Lantmäteriverket. Detta ökar risken för brister i ledningssystemets funktion och därmed i informationssäkerheten.

7 Uppföljning och förvaltning

7.1 Bedömningskriterier

Den snabba förändringstakten i Lantmäteriverkets omvärld 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 skyddsåtgärder:
  – genomförande av åtgärdsplanerna
  – incidentrapporteringen
  – kontinuitetsplaneringen
  – den interna kontrollen av utveckling/förändringar i IT-miljö, IT-system och bemanning
  – den interna kontrollen av tekniska skyddsåtgärders funktion (behörighetskontrollsystem, virusskydd, brandväggar m.m.)
  – om den faktiskt uppnådda informationssäkerheten systematiskt prövas och uppfyller säkerhetskraven
- Information/utbildning: den interna kontrollen beträffande 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

I Lantmäteriverkets riktlinjer[41] specificeras vilken dokumentation som ska finnas avseende informationssäkerhet. Det har emellertid inte gjorts någon uppföljning av att förtecknade riktlinjer, planer och analyser har tagits fram. I styrkorten till 2006 års verksamhetsplan ingår emellertid att risk- och sårbarhetsanalyser ska göras för de viktigaste systemen.

Lantmäteriverket har i en processbeskrivning[42] regler för att särskilt allvarliga incidenter ska rapporteras till IT-säkerhetsansvarig. Här anges även att uppföljning av den övergripande processen för incidenthantering ska ske genom avrapportering från IT-säkerhetsansvarig, t.ex. till säkerhetschefen. Någon uppföljning av fullständigheten i rapporterade incidenter har dock inte skett.

Lantmäteriverket har inte någon **systematisk och regelbunden** uppföljning av sitt ledningssystem för informationssäkerhet. Det finns heller ingen **dokumenterad** process för uppföljning, förvaltning och utveckling av informationssäkerhetsarbetet.

Ledningen har valt en starkt delegerad organisation för informationssäkerhetsarbetet inom Lantmäteriet. Det saknas dock en systematisk uppföljning från ledningens sida av om beslutade **delegationer** fungerar som avsett. Det blir därmed svårt för ledningen att få en samlad bild av hur väl informationssäkerheten fungerar.

Internrevisionen inom Lantmäteriverket har gjort två granskningar som rör informationssäkerhet inom Lantmäteriet: en granskning 2001[43] om IT-säkerhet och generella kontroller och en under 2006[44] avseende incidenthantering. Båda granskningarna avsåg koncerngemensamma interna stödsystem. Lantmäteriverket har successivt arbetat med att åtgärda iakttagelserna från granskningen 2001, t.ex. har placeringen av IT-säkerhetsfunktionen förändrats till att bli mer central. Dock kvarstår internrevisionens rekommendationer om att uppdatera riktlinjerna. När det gäller rapporten från 2006 har Lantmäteriverket angett att riktlinjer och rutiner ska ses över.

Under intervjuerna har det inte entydigt framgått vem som faktiskt ansvarar för uppföljning av informationssäkerhetsarbetet inom Lantmäteriverket. I enlighet med *Riktlinjerna för informationssäkerhet* har säkerhetschefen ett ansvar för uppföljning, men i praktiken har IT-säkerhetsfrågorna delegerats till IT-informationssäkerhetsansvarig. Det är inte specificerat vad det delegerade ansvaret innebär. Detta medför att uppföljningen brister både av beslutade komponenter och av ledningssystemet som helhet.

---

[41] Riktlinjer för informationssäkerhet, Lantmäteriverket 1999-02-15, kap. 7.
[42] Processen för hantering av IT-incidenter (ITS03), 2003-01-20.
[43] IT-säkerhet Generella kontroller, 2001-12-14, dnr 203-2001/2455.
[44] Incidenthantering koncerngemensamma system 2006-02-10, dnr 203-2005/1218.

7.3 Bedömning

Riksrevisionen bedömer att det finns brister i uppföljningen av de delar av ledningssystemet för informationssäkerhet som Lantmäteriverket har etablerat. Den uppföljning som görs är till stor del händelsestyrd och det saknas en systematisk uppföljning av hur ledningssystemet fungerar.

Eftersom det är oklart vem som är ansvarig för ledningens uppföljning och det finns brister i uppföljningen blir det svårt för ledningen att på ett strukturerat sätt prioritera och fatta beslut om förbättringar i arbetet med informationssäkerheten.

Sammantaget bedömer Riksrevisionen att bristerna i uppföljning och förvaltning av ledningssystemet riskerar att påverka informationssäkerheten negativt.

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 Lantmäteriverkets myndighetsledning tar sitt ansvar för informationssäkerheten.

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

8.1 Slutsatser

Vid Lantmäteriverket finns flera fungerande delar av ett ledningssystem för informationssäkerhet. Det finns ett antal styrdokument som är beslutade och tillgängliga. Lantmäteriverket har på en lägre organisatorisk nivå genomfört ett stort antal skyddsåtgärder. Lantmäteriverkets ledning har uppmärksammat problemet med otydligheter kring vilka system man har, vem som är systemägare och behovet av fungerande reservdriftsrutiner. Detta har lett till att konkreta och tydliga åtgärder tagits upp i verksamhetsplaneringen för 2006. De planerade åtgärderna har även följts upp av ledningen under året.

Granskningen visar dock att Lantmäteriverkets ledningssystem för informationssäkerhet inte är tillräckligt tydligt utformat. Ledningen har inte skapat en tydligt fungerande helhet i systemet och har därmed, enligt Riksrevisionens bedömning, inte tillräckligt stöd eller hjälpmedel för att skapa överblick samt leda och följa upp informationssäkerheten. Bristerna gäller framför allt att det finns oklarheter i ansvarsfördelningen, att riskanalysarbetet inte har fullföljts samt att uppföljningen inte är systematisk.

Bristerna försvårar ledningens möjligheter att säkerställa att verksamhetens olika delar arbetar systematiskt och med samma ambitionsnivå avseende informationssäkerheten. Det medför risk för att informationssäkerheten befinner sig på olika nivåer inom myndigheten utan att detta varit ledningens avsikt. Det försvårar även möjligheterna att samla erfarenheter och utveckla ledningssystemet. Därmed ökar risken för en sämre informationssäkerhet vid Lantmäteriverket.

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

arbetar systematiskt med sitt ledningssystem för informationssäkerhet. Bedömningen baseras på tre huvudsakliga brister. Bristerna har redan beskrivits mer ingående i de tidigare kapitlen. Nedan sammanfattas beskrivningen av brister.

8.1.1 Oklar ansvarsfördelning

Det finns oklarheter på centrala punkter vad gäller ansvarsfördelningen inom arbetet med informationssäkerhet. Oklarheterna avser framför allt IT-säkerhetsansvarig, systemägare och förvaltningsansvarig. Utformningen av vissa ansvarsroller skiljer sig dessutom åt mellan de tre divisionerna inom Lantmäteriverket. Därmed är ansvarsrollerna inte tillräckligt tydligt beskrivna eller etablerade vid Lantmäteriverket.

Det finns ingen systematisk utbildningsprocess för att säkerställa att nyckelpersoner inom säkerhetsarbetet erhåller tillräcklig och återkommande utbildning inom området.

Detta innebär en risk för att arbetsuppgifter inom området informationssäkerhet vid Lantmäteriet utförs på olika sätt inom organisationens olika delar. Det finns också en risk att säkerhetsåtgärder inte utförs.

8.1.2 Riskanalysarbetet har inte fullföljts

Riskanalys är en viktig förutsättning för och del av myndighetens riskhantering. De centrala kraven på riskanalyser har varit otydliga inom Lantmäteriverket. Ingen uppföljning av riskanalyser har tidigare genomförts vid Lantmäteriverket, men under 2006 har en sådan process påbörjats.

Lantmäteriverket har i sina riskanalyser inte fullt ut beaktat systemsamverkan[45] och de krav som därav följer vid analyser av t.ex. behov och utformning av möjligheter till reservdrift. Ett exempel på detta är särskilt de olika förmågor man har till reservdrift i stordatormiljö jämfört med de nyare åtkomstsystemen i Unix-miljö. Ett arbete har under 2006 påbörjats för att förbättra reservdriften i Unix-miljön.

Klassificering av information som grund för prioritering av skyddsåtgärder är endast till vissa delar genomförd; detta avser framför allt den information som är av totalförsvarskaraktär. Det finns ingen beslutad modell för klassificering av information; dock finns förberedande analyser av tillgänglighetsbehov för kart- och fastighetsinformation.

[45] Med systemsamverkan avses här att ett system är beroende av andra omgivande system.

8.1.3 Uppföljningen är inte systematisk

Det finns ingen tydligt utpekad ansvarig för uppföljning av införandet av säkerhetsåtgärder vid Lantmäteriverket. Flera styrdokument som behandlar informationssäkerhet är inaktuella. Ingen systematisk sammanställning eller uppföljning görs av de IT-incidenter som förekommer inom Lantmäteriet (större incidenter förs dock upp till ledningens kännedom). Ledningens uppföljning av informationssäkerheten är till stor del reaktiv och händelsestyrd. De proaktiva inslagen – dvs. uppföljning av de beslutade åtgärderna och deras genomförande – är sparsamt förekommande[46]. Ledningen bedöms därför inte ha ett tillräckligt underlag för att göra en tillförlitlig uppföljning av gjorda delegationer. Brister i uppföljningen påverkar också negativt vidareutvecklingen av Lantmäteriverkets ledningssystem för informationssäkerhet.

8.2 Rekommendationer

Riksrevisionens bedömning är att ett sammanhållet och tydligt ledningssystem för informationssäkerhet är en förutsättning för att Lantmäteriverkets ledning ska kunna förvissa sig om att beslutade säkerhetsnivåer införs och bibehålls i hela myndigheten. Detta kräver bl.a. att ledningssystemet stärker ledningens möjligheter till överblick av risker och skillnaderna i risker mellan olika verksamheter, behovet av säkerhetsåtgärder och kostnaderna för säkerhetsarbetet i de olika verksamheterna. Då framstår också tydligare vilket utrymme som finns för prioriteringar av säkerhetsinvesteringar i skilda delar av myndigheten. Ledningssystemet bör därför vara giltigt för hela Lantmäteriet 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.

Brister i informationssäkerheten hos Lantmäteriverket kan leda till att åtkomsten till geografisk information och fastighetsinformation försämras eller uteblir. Detta kan i sin tur ge allvarliga konsekvenser hos stora användare. Exempelvis kan enskilda drabbas eftersom fastighetsregistret ligger till grund för bankers och kreditinstituts långivning.

[46] De förekommer dock, t.ex. åtgärder att kartlägga system, systemägare och behov av reservdrift enligt verksamhetsplan för 2006.

Riksrevisionen rekommenderar därför Lantmäteriverket följande:

- Lantmäteriverket bör tydligare beskriva och kommunicera till organisationen hur ledningssystemet för informationssäkerhet ska fungera för att stärka ledningens möjligheter enligt ovan. I detta arbete med att införa ett ledningssystem för informationssäkerhet ligger även att precisera och etablera en tydlig ansvarsfördelning.
- Lantmäteriverket bör besluta hur riskanalysarbete, samlad planering av säkerhetsåtgärder samt uppföljning av arbetet med informationssäkerhet ska bedrivas. Lantmäteriverket bör även införa en systematisk uppföljning och dokumentation av IT-incidenter.
- Lantmäteriverket bör fullfölja sin planerade genomgång av system, systemägare och behovet av reservdriftsrutiner som en grund för det fortsatta arbetet med informationssäkerheten. Det fortsatta arbetet bör även inbegripa att förteckna informationstillgångarna.

Källförteckning

Lagar

Arkivlag (1990:782)

Lag (2003:389) om elektronisk kommunikation

Personuppgiftslag (1998:204)

Sekretesslag (1980:100)

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

Säkerhetsskyddslag (1996:627)

Förordningar

Arkivförordning (1991:446)

Förordning (2006:942) om krisberedskap och höjd beredskap

Förordning (1995:1300) om myndigheters riskhantering

Personuppgiftsförordning (1998:1191)

Säkerhetsskyddsförordning (1996:633)

Tryckfrihetsförordning (1949:105)

Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap

Verksförordning (1995:1322)

Förordning (1995:1418) med instruktion för det statliga lantmäteriet

Föreskrifter och allmänna råd

Datainspektionens allmänna råd: Säkerhet för personuppgifter (december 1999)

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

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

Krisberedskapsmyndigheten 2006. Krisberedskapsmyndighetens rekommendation 2006:1 Basnivå för informationssäkerhet (BITS), utgåva 3

Standarder

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

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

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

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

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

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

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

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

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

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

SP800-40 *Procedures for Handling Security Patches,*

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

SP800-42 *Guideline on Network Security Testing,*

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

SP800-45 *Guidelines on Electronic Mail Security,*

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

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

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

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

SP800-55 *Security Metrics Guide for Information Technology Systems,*

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

SP800-61 *Computer Security Incident Handling Guide,*

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

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

Texter från Internet

Mörkertalsundersökningen. Hämtad från http://www.pts.se/Archive/Documents/SE/Morkertalsundersokningen_2005.pdf

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

· *Draft Special Publication 800-40 Version 2 – Creating a Patch and Vulnerability Management Program*
· *Draft NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling*
· *NIST DRAFT Special Publication 800-26, Revision 1: Guide for Information Security Program Assessments and System Reporting Form*

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

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 Granskning av Arbetsmarknadsverkets interna styrning och kontroll av informationssäkerheten
2006: 25 Granskning av Migrationsverkets interna styrning och kontroll av informationssäkerheten

Beställning: publikationsservice@riksrevisionen.se