Post- och telestyrelsen
Box 5398
102 49 Stockholm

Datum 2006-02-09
Dnr 32-2005-0738

Post- och telestyrelsens informationssäkerhet

Riksrevisionen har som ett led i den årliga revisionen av Post- och telestyrelsen (PTS) granskat myndighetens ledningssystem för informationssäkerhet (LIS).

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

Riksrevisionen önskar information senast 2006-04-10 med anledning av våra iakttagelser i denna rapport.

1. Inledning

I takt med att inslagen av elektronisk förvaltning ökar hos de flesta statliga myndigheter och allt större krav ställs på att e-tjänsterna är säkra, inte minst för att medborgare och företagare ska ha förtroende för dessa tjänster, ökar också kraven på en god informationssäkerhet. Med denna utveckling följer att myndigheterna behöver se över och vid behov förstärka sitt informationssäkerhetsarbete för att bringa detta i paritet med den förändrade riskbilden som följer bl.a. av den elektroniska förvaltningen.

I denna granskning har tyngdpunkten legat på myndighetsledningens interna styrning och kontroll för att säkerställa skyddet av PTS IT-relaterade informationstillgångar. Denna styrning och kontroll benämns vanligen samlat som Ledningssystem för informationssäkerhet (LIS). Avgränsningen innebär att faktiskt uppnådd säkerhet i enskilda system inte har granskats.

Den huvudsakliga normkällan för de bedömningar som gjorts vid granskningen har varit standarden Ledningssystem för informationssäkerhet (SS 627799 och SS-ISO/IEC 17799).

De bedömningsnormer som använts har i rapporten strukturerats efter kontrollkomponenterna i den interna styrningen och kontrollen i enlighet med

COSO-modellen[1]. Enligt COSO-modellen omfattar intern kontroll följande delar:

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

En beskrivning av bedömningskriterierna för respektive komponent inleder respektive avsnitt nedan.

2. PTS och informationssäkerhet

2.1 Allmänt

PTS har i delar av sin verksamhet ett högt beroende av väl fungerande informationssäkerhet, bl.a. i form av hantering av material som kan omfattas av sekretess.

Vår bedömning är att PTS har saknat ett samlat och strukturerat förhållningssätt till informationssäkerhetsfrågor. PTS har dock under hösten 2005 initierat ett arbete med att införa en styrning av informationssäkerhetsarbetet utifrån etablerade standards. Detta arbete utgår i allt väsentligt från den standard som beskrivits ovan (SS 627799 och SS-ISO/IEC 17799). Vid granskningstillfället pågick ett inledande arbete med riskanalys och informationsklassificering i organisationen, vilket därefter är tänkt att leda till att grunderna för införandet av ett LIS kan etableras.

Ett antal åtgärder i form av styrande dokument, tekniska skyddslösningar etc. har sedan tidigare införts i organisationen, men dessa tycks inte ha varit resultatet av någon samlad analys av verksamhetens faktiska behov. Vissa grundläggande moment som normalt bör ingå i en myndighets informationssäkerhetsarbete tycks inte ha beaktats, exv. en heltäckande förteckning och klassificering av myndighetens informationstillgångar. Vi har inte heller funnit något dokumenterat ställningstagande till eventuellt behov av kontinuitetsplanering för verksamheten.

Ett antal styrande dokument som kan ses som viktiga komponenter i LIS saknas för närvarande vid PTS. Denna rapport har inriktat sitt innehåll på att beskriva vilka komponenter som normalt bör ingå i LIS, samt på vilka punkter vi anser att PTS särskilt kan förstärka sitt arbete med styrning av informationssäkerhetsarbetet.

[1] 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.

Nedan redovisas kortfattat vissa kriterier som legat till grund för våra bedömningar, vilket också kan ses som ett stöd i samband med att myndigheten ska implementera ett ledningssystem för informationssäkerhet.

2.2 Kontrollmiljö

Bedömningskriterier

Kontrollmiljön är en del av myndighetskulturen och skapas av myndighetens chefer. En god kontrollmiljö kännetecknas av:

- Ett tydligt visat engagemang från ledningen.
- En från ledningen kommunicerad syn på betydelsen av intern styrning och kontroll av informationssäkerheten, vilket kan ske i en informationssäkerhetspolicy.
- Att ledningen skapat tillräckliga resurser för arbetet med informationssäkerheten.
- Inrättandet av tydliga funktioner – periodiska genomgångar, säkerhetsansvarig (controller), rapporteringsrutiner m.m. – för att kontrollera om organisationen av informationssäkerheten och införda säkerhetsåtgärder fungerar enligt ledningens intentioner och beslut.

Iakttagelser och bedömningar från granskningen

Vi har noterat att PTS saknar flera av de formella dokument och rutiner som normalt behövs för att säkerställa en god kontrollmiljö i enlighet med de bedömningskriterier som nämnts ovan; bl.a. policy för användning av e-post, avbrotts- och kontinuitetsplaner m.m.. Det är vidare oklart på vilket sätt de policydokument avseende säkerhet och informationssäkerhet som funnits tillgängliga har införts i organisationen. Vi bedömer även att det i dagsläget saknas tydliga uppföljningsfunktioner som visar om ledningens intentioner inom området följs.

Det ska i sammanhanget nämnas att PTS har vissa dokument där ledningens intentioner rörande informationssäkerhet framgår, bland annat en säkerhetsstrategi och riktlinjer för informationssäkerhet. Genomförda intervjuer indikerar dock att det är tveksamt om myndigheten har något samlat grepp om arbetet med informationssäkerhetsfrågor.

PTS har noterat brister inom området och arbetar för tillfället med att åtgärda detta, bl.a. pågår arbete med utformning av en ny informationssäkerhetspolicy samt utformning av en organisation för kontinuerligt informationssäkerhetsarbete.

Vi vill särskilt poängtera behovet av ett tydligt ledningsengagemang i informationssäkerhetsfrågorna, vilket också bör avspegla sig i informationssäkerhetspolicyn med därtill kopplade uppföljningsfunktioner.

2.3 Riskanalys

Bedömningskriterier

Riskhantering är aktiviteter på ledningsnivå som bör omfatta en process för systematisk riskanalys - innebärande att de utförs med hjälp av beslutade systematiska[2] och dokumenterade metoder. Denna process omfattar analyser och bedömningar av väsentliga hot, risker och konsekvenser.

Vidare bör det finnas en åtgärdsplan som förtecknar beslutade åtgärder för att möta de risker som framkommit i analysen t.ex. avbrottsplanering, förstärkning av skyddsåtgärder, skadefinansiering och eventuellt försäkringsskydd. Planen bör beskriva när åtgärderna ska vara genomförda och vilka som ansvarar för deras genomförande. Genomförandet bör följas upp.

Som underlag för analysen behövs identifiering[3] av de skyddsvärda informationstillgångarna. De bör dokumenteras i en överblickbar förteckning. Åtminstone de tillgångar som är strategiska för verksamheten bör åsättas en beslutad säkerhetsnivå[4] – klassning - med hänsyn till verksamhetens krav på tillgänglighet, riktighet och sekretess så att en prioritering av åtgärder kan göras.

Riskanalys bör årligen och däremellan vid behov uppdateras.

Iakttagelser och bedömningar från granskningen

För närvarande saknar PTS, enligt vår bedömning, en metodisk process för analys av vilka informationstillgångar som är mest verksamhetskritiska och skyddsvärda för myndigheten, samt vilka risker som finns avseende berörda tillgångar. Nuvarande klassificering av myndighetens informationstillgångar utgår i princip endast från ett av de kriterier som angivits ovan, sekretesskravet. Detta medför att myndigheten riskerar att kritiska tillgångar inte erhåller tillräckligt hög skyddsnivå, samt att säkerhetshöjande insatser sker utifrån fel prioriteringar.

---

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

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

[4] Ett sätt att prioritera är att utifrån ledningens syn på konsekvenser av brister ange klasser i olika nivåer (t.ex. Mycket kritiskt, Viktigt, Mindre viktigt).

PTS har under hösten 2005 initierat ett arbete med riskanalys och informationsklassificering, som kan ligga till grund för fortsatt arbete inom informationssäkerhetsområdet.

2.4 Ledningens kontrollfunktioner

Bedömningskriterier

Kontrollfunktioner är i detta sammanhang dels åtgärder som ledningen utformat för att förebygga, upptäcka och åtgärda brister i informationssäkerheten, dels enskilda säkerhetsåtgärder som syftar till att skydda informationstillgångar eller skydda själva säkerhetsåtgärden. Kontrollfunktionerna utgör sammantaget myndighetens ledningssystem för informationssäkerhet (LIS).

Det bör finnas en till all personal kommunicerad skriftlig beskrivning av roller[5] i informationssäkerhetsarbetet och hur ansvar och befogenheter för myndighetens informationssäkerhet fördelats på dessa. Vidare bör alla medarbetares eget ansvar framgå.

LIS bör om inte särskilda skäl[6] finns omfatta följande komponenter[7]:

- Informationssäkerhetspolicy
- Process för incidentrapportering inkl. 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[8]
- Process för säkerhetskopiering av all verksamhetskritisk information
- Process för styrning av utveckling/förändringar i IT-miljö, IT-system och bemanning
- Processer för återkommande uppföljning och förvaltning av LIS

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

[6] Om det exempelvis inte sker något distansarbete så behövs givetvis ingen distansarbetspolicy.

[7] 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

[8] Policy som reglerar åtkomst av informationstillgångar

Dessa bör vara dokumenterade, beslutade och införda i verksamheterna. De bör vara utformade utifrån myndighetens särskilda behov och därvid beakta relevant best practice[9] inom aktuellt område.

Komponenterna bör utgöra en lämpligt utformad helhet – som i sin tur bör utgöra en integrerad del i myndighetens totala ledningssystem.

Iakttagelser och bedömningar från granskningen

Granskningen visar att PTS infört ett antal tekniska säkerhetsåtgärder i sin IT-infrastruktur (behörighetskontrollsystem, virusskydd, brandväggar m.m.) för att skydda sina informationstillgångar. Som tidigare nämnts saknas dock flera av de grundläggande komponenterna som bör utgöra en del av myndighetens ledningssystem. Bland annat saknas policy för e-postanvändning, policy för styrning av åtkomst, övergripande kontinuitetsplanering samt rutiner för uppföljning och förvaltning av informationssäkerhetsarbetet.

Vi har också i samband med granskningen konstaterat att vissa rutiner idag inte tillämpas på tillfredsställande sätt (se Riksrevisionens revisionspromemoria daterad 2006-01-30, dnr 32-2005-0738). T.ex. noterades att ett stort antal användare hade omfattande behörigheter att såväl ändra som ta bort information i lönesystemet. Bland användare med dessa behörigheter fanns även personer som inte längre är anställda vid myndigheten.

2.5 Information och utbildning

Bedömningskriterier

Information avser ledningens åtgärder för att förse personalen med relevant information och kunskaper angående myndighetens informationstillgångar, säkerhetsåtgärder, incidenter och ledningssystem för informationssäkerhet.

Det bör finnas en process för systematisk och återkommande information och utbildning beträffande informationssäkerhet till relevanta grupper[10]. Den bör innefatta de anställdas ansvar för informationssäkerheten samt de väsentliga hot och risker som ska beaktas i deras arbete.

Vidare bör det finnas en process för återkommande uppföljning av att IT-användarna är tillräckligt medvetna om och kompetenta att hantera hot och risker.

---

[9] Myndigheten ska alltså informera sig om och dra nytta av de kunskaper som finns i standards såsom SIS 17799, NISTs 800-serie av rapporter mfl.

[10] Nyanställda, myndighetsledning, övriga chefer, övriga medarbetare.

Iakttagelser och bedömningar från granskningen

Idag ingår PTS säkerhetsfrågor som en del i introduktionsutbildningen av de nyanställda. Under december 2005 har också en särskild informationsdag hållits för personalen angående informationssäkerhetsfrågor.

Det är viktigt att PTS fortlöpande tillser att personalen har tillräckliga kunskaper om informationssäkerheten och de regler som finns, och att denna kunskap uppdateras regelbundet, exv. genom återkommande informationsträffar, utbildning etc.

2.6 Uppföljning och förvaltning

Bedömningskriterier

Uppföljningen bör vara en naturlig del av ledningens kontroll av att delegerad befogenhet hanteras på avsett sätt. Uppföljningen bör ske systematiskt och regelbundet genom av ledningen inrättade funktioner. Vid vissa tillfällen kan därutöver särskilda insatser vara påkallade i form av konsultuppdrag och andra utvärderings/kontrollinitiativ. Sådana insatser kan emellertid inte ersätta den systematiska och regelbundna uppföljningen.

Uppföljningen bör avse de kontrollobjekt som är av större betydelse för informationssäkerheten i myndighetens verksamhet såsom att

- riskanalysprocessen fungerar som avsett.
- åtgärdsplanering och genomförande fungerar som avsett.
- incidentrapporteringen fungerar som avsett.
- kontinuitetsplaneringen fungerar som avsett.
- e-posthanteringen fungerar som avsett.
- den interna kontrollen av förändringar i IT-miljön och personella resurser fungerar som avsett.
- den interna kontrollen av åtkomst av informationsresurser fungerar som avsett.
- distansarbetspolicyn fungerar som avsett.
- internetpolicyn fungerar som avsett.
- information och utbildning betr. informationssäkerhet fungerar som avsett.
- den faktiskt uppnådda informationssäkerheten systematiskt prövas och uppfyller säkerhetskraven.

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

Iakttagelser och bedömningar från granskningen

Granskningen visar att PTS idag inte har en dokumenterad process för förvaltning och uppföljning av sitt LIS. Ledningen är medveten om detta och den projektgrupp som nu arbetar med att etablera grunder för ett införande av LIS vid PTS har bl.a. till uppgift att ta fram förslag till organisation samt handlingsplaner för samordning och kontroll för arbetet med informationssäkerhetsfrågor.

Det är dock viktigt att PTS tillser att tillräckliga resurser avsätts, även efter att det pågående projektet avslutats, för att informationssäkerhetsarbetet kontinuerligt kan vidareutvecklas och förvaltas. En viktig del av detta arbete är att resurser avsätts för regelbunden uppföljning av att ledningens intentioner inom informationssäkerhetsområdet efterlevs av organisationen.

3. Slutsatser och rekommendationer

PTS verksamhet omfattar hantering av ärenden som är sekretessbelagda, och även annan kritisk verksamhetsinformation.

Granskningen av PTS ledningssystem för informationssäkerhet visar att myndigheten infört ett antal komponenter i sitt LIS som bör finnas enligt standarden Ledningssystem för informationssäkerhet (SS 627799 och SS-ISO/IEC 17799). Det gäller konkreta skydd av informationstillgångar, t.ex. behörighetssystem, skalskydd, säkerhetskopiering etc. Myndigheten har också utarbetat vissa policydokument och riktlinjer.

Riksrevisionen har dock sammanfattningsvis gjort följande iakttagelser:

- Den osäkerhet som tycks råda om status på nuvarande informationssäkerhetspolicy, innebär att ledningen inte till fullo kommunicerat sin helhetssyn avseende vikten av informationssäkerhet. Detta återspeglas även genom att det inte finns några formellt fastställda krav avseende kontinuitetsplanering, rutiner för incidentrapportering, e-postanvändning m.m. vid myndigheten. Det har också saknats en fördelning av roll- och ansvar avseende informationssäkerhetsarbetet. Denna fråga adresseras delvis i en förvaltningsmodell som beslutats i oktober 2005, men denna kan behöva vidareutvecklas ytterligare, beroende på utfallet av nu pågående utredning av myndighetens informationssäkerhet.
- PTS har först under hösten och vintern 2005 genomfört en riskanalys och heltäckande informationsklassificering av myndighetens informationstillgångar, vilket är en grundläggande förutsättning för en effektiv riskhantering vid myndigheten. Det är viktigt att nivån och omfattningen av såväl organisatoriska och tekniska kontroller rörande verksamhetens informationstillgångar baseras, dels på ovan nämnda ställningstagande och inriktningsbeslut från ledningen, dels på utfallet av en strukturerad process för riskanalys och

informationsklassificering. Detta innebär i praktiken att verksamhetsföreträdare och myndighetsledningen måste ta ansvar för att bedöma vilken nivå av kontroller och informationsskydd som krävs.

- Vi har även noterat att ledningens uppföljnings- och kontrollrutiner inte varit tillfredsställande avseende LIS. Vi vill poängtera vikten av att informationssäkerhetsarbetet ses som en kontinuerlig process. Detta innebär bl.a. att det bör finnas en modell för (och resurser avsatta till) kontinuerlig prövning och värdering av myndighetens informationssäkerhetsarbete. Detta dels genom regelbunden omprövning av tidigare riskanalyser, dels genom uppföljande åtgärder för att bedöma om införda kontroller fungerat på avsett sätt. Det bör även finnas en plan för att säkerställa att all personal på lämpligt sätt får tillgång till uppdaterad information om myndighetens övergripande ställningstaganden i informationssäkerhetsfrågor, och inte minst det ansvar som åvilar den enskilde.

Vi *rekommenderar* PTS att tillse att noterade brister i ledningssystemet för informationssäkerheten blir åtgärdade. Detta är särskilt viktigt med tanke på den roll och de uppgifter PTS har inom informationssäkerhetsområdet. Vi vill särskilt betona att identifieringen av skyddsvärda informationstillgångar samt riskanalys, som PTS nu genomför är en viktig grund för införandet av kontroller och skyddsåtgärder i verksamheten, men att dessa regelbundet måste värderas och omprövas i en återkommande process.

Revisionsledare Frank Lantz har beslutat i detta ärende. Revisionsledare Carina Franzén har varit föredragande.

Frank Lantz Carina Franzén

Kopia för kännedom:

Näringsdepartementet

Finansdepartementet/budgetavdelningen