Bolagsverket
851 81 SUNDSVALL

Datum 2005-08-19
Dnr 32-2005-0717

Bolagsverkets informationssäkerhet

Riksrevisionen har som ett led i den årliga revisionen av Bolagsverket granskat ledningssystemet för informationssäkerhet (LIS).

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

Riksrevisionen önskar information senast 2005-09-19 med anledning av våra iakttagelser i denna rapport.

generellt genom att motiven till de viktiga komponenterna beskrivs.

1. Inledning

Informationssäkerheten är väsentligt i tiden därför att elektronisk förvaltning får insteg 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. Med denna utveckling följer bl.a. 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 granskningen har tyngdpunkten legat på myndighetsledningens interna styrning och kontroll för att säkerställa säkerheten/skyddet av Bolagsverkets IT-relaterade informationstillgångar. Denna styrning och kontroll benämns samlat för ledningssystem för informationssäkerhet (LIS). Avgränsningen innebär bl.a. att faktiskt uppnådd säkerhet i enskilda system inte granskats.

Standarden Ledningssystem för informationssäkerhet har varit den huvudsakliga normkällan.

Normerna 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 komponenter:

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

[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.

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

2. Bolagsverket och informationssäkerhet

2.1 Allmänt

Bolagsverkets IT-beroende är mycket högt och omfattningen av e-tjänster och exponering på Internet är även den mycket stor.

Bolagsverkets egen uppfattning om informationssäkerheten är att den är tillräcklig, men att det finns brister i ledningssystemet för informationssäkerheten. Anledningen till dessa brister kan förklaras av att myndigheten är nystartad. Bolagsverket har valt att bygga upp sin verksamhet avseende policys och andra styrande dokument – även beträffande LIS – från grunden utan att ta hänsyn till det som funnits tidigare under PRV-tiden. Av den anledningen saknas alltså en rad styrande dokument som kan ses som viktiga komponenter i Ledningssystemet för informationssäkerhet. Denna rapport har inriktat sitt innehåll på att beskriva vilka komponenter som bör ingå och varför.

Nedan redovisas vad som legat till grund för våra bedömningar vilket också kan ses som ett stöd i samband med att myndigheten ska implementera ett ledningssystem för informationssäkerheten.

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

Vi har noterat att Bolagsverket saknar vissa formella dokument och rutiner för att säkerställa en god kontrollmiljö i enlighet med de bedömningskriterier som nämnts ovan. Framförallt avsaknaden av en informationssäkerhetspolicy, där ledningen kan uttrycka sina krav på informationssäkerhet, samt avsaknaden av tydliga uppföljningsfunktioner som visar att ledningens intentioner följs.

Det ska i sammanhanget nämnas att Bolagsverket har en rad dokument och policys där ledningens intentioner rörande informationssäkerhet framgår. Bland annat policys rörande Internet och e-postanvändande, distansarbetspolicy, systemutvecklingsmodeller och projektstyrningsmodeller etc. Ledningens instrument för att i dag försäkra sig om att informationssäkerheten fungerar som tänkt sker med hjälp av informella rapporteringsrutiner.

Ledningen är som sagt väl medveten om dessa brister och planerar för tillfället hur man ska åtgärda detta.

Vi har noterat ett engagemang från ledningen rörande dessa frågor. Detta engagemang bör också avspegla sig i en informationssäkerhetspolicy med 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. Den 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 bedömning

Bolagsverket saknar en riskanalys. Det saknas också en förteckning över informationstillgångarna där säkerhetsnivån har klassats. Ledningen har för avsikt att tillsätta ett projekt som ska ha till uppgift att göra en klassificering av informationstillgångarna. Denna ska ligga till grund för en riskanalys.

---

[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).

Avsaknaden av en metodisk process för analys av informationssäkerhetsrisker medför svårigheter med att skapa ett fullgott underlag för beslut som avser hanteringen av riskerna.

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 sammantagna 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

De 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.

---

[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

[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.

Komponenterna bör utgöra en lämpligt utformad helhet – ett ledningssystem som bör utgöra en integrerad del i myndighetens ledningssystem.

Iakttagelser och bedömningar

Granskningen visar att Bolagsverket infört ett antal tekniska säkerhetsåtgärder i sin IT-infrastruktur (behörighetskontrollsystem, virusskydd, brandväggar m.m.) för att skydda sina informationstillgångar. Som tidigare nämnts saknas dock ett flertal av de ovan angivna komponenterna som ska utgöra en del av myndighetens ledningssystem. Bland annat informationssäkerhetspolicy, process för incidentrapportering, åtgärdsplaner och en övergripande kontinuitetsplaner etc.

2.5 Information och utbildning

Bedömningskriterier

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

Det bör finnas en process för systematisk och återkommande information och utbildning betr. 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.

Iakttagelser och bedömningar

Idag genomför Bolagsverket informationssäkerhetsutbildning för olika personalkategorier som en del i introduktionsutbildningen av de nyanställda. Vissa i ledningen deltar i vissa nätverk i syfte att upprätthålla en viss omvärldsbevakning.

I samband med att Bolagsverket utarbetar policys eller dylikt har de också behandlats på arbetsplatsträffar där personalen har chans att lämna synpunkter. Detta är ett utmärkt sätt att få återkoppling samtidigt som man informerar och utbildar i ämnet.

Vi bedömer att Bolagsverket framledes bör inrätta funktioner som skapar garantier för att personalen har tillräckliga kunskaper om informationssäkerheten och följer de regler som finns. Avsaknaden av dylika funktioner ökar på ett oberäkneligt sätt risken för brister i informationssäkerheten.

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

2.6 Uppföljning och förvaltning

Bedömningskriterier

Uppföljningen bör vara en naturlig del av ledningens uppföljning av den valda delegationen av sitt ansvar. Uppföljningen bör ske systematiskt och regelbundet genom av ledningen inrättade funktioner såsom internrevision och säkerhetscontroller. 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

Granskningen visade att Bolagsverket inte har en dokumenterad process för förvaltning och utveckling av sitt LIS. Ledningen är väl medveten om detta och det pågår ett arbete med att tillsätta en projektgrupp som har för avsikt att identifiera verkets informationstillgångar, vilket kan ses som ett startskott för denna process.

3. Slutsatser och rekommendationer

Myndighetens utveckling av e-tjänster har lett till en ökad exponering för risker för andra aktörer och myndigheter som är beroende av den information som förmedlas via de nya e-tjänsterna. Denna ökade risk är Bolagsverket väl medveten om.

Granskningen av Bolagsverkets ledningssystem för informationssäkerhet visar att myndigheten infört ett flertal komponenter i sitt LIS enligt standarden SIS 17799. Det gäller konkreta skydd av informationstillgångar, t.ex. behörighetssystem, eget skalskydd, säkerhetskopiering etc. Myndigheten har också utarbetat vissa policys avseende e-post och Internet samt distansarbete. Det ska också nämnas att Bolagsverket har för avsikt att använda sig av Statsverkets modell för LIS avseende statsförvaltningen (OFF-LIS)

Riksrevisionen har sammanfattningsvis gjort följande iakttagelser och konsekvensbeskrivningar:

- Avsaknaden av en övergripande styrande policy, såsom en informationssäkerhetspolicy, innebär att ledningen inte kommunicerat sin helhetssyn avseende vikten av informationssäkerhet. Detta innebär bland annat att det inte finns några krav avseende kontinuitetsplan, incidentrapportering, virusskydd etc. Det saknas också en fördelning av roll- och ansvar avseende informationssäkerheten.
- Bolagsverket har inte genomfört någon riskanalys, vilket är en viktig förutsättning för myndighetens riskhantering. Avsaknaden av en metodisk process för analys av informationssäkerhetsrisker medför svårigheter med att skapa ett fullgott underlag för beslut som avser hanteringen av riskerna.
- Vi har även noterat brister i ledningens uppföljnings- och kontrollrutiner, information och utbildning samt förvaltningen av LIS. Detta bedömer vi som en följd av det inte genomförts någon övergripande riskanalys samt avsaknaden av en informationssäkerhetspolicy.

Vi *rekommenderar* Bolagsverket att tillse att de noterade bristerna i ledningssystemet för informationssäkerheten blir åtgärdade. Vi anser att identifieringen av skyddsvärda informationstillgångar, som Bolagsverket planerar, samt efterföljande riskanalys bör genomföras i närtid.

Roland Fellman

Kopia för kännedom:

Näringsdepartementet

Finansdepartementet/budgetavdelningen