Revisionsrapport

RIKSREVISIONEN

Skogsstyrelsen
551 83 Jönköping

Datum 2011-02-08
Dnr 32-2010-0672

Uppföljande granskning av Skogsstyrelsens interna styrning och kontroll av informationssäkerhetsarbetet

Riksrevisionen har som ett led i den årliga revisionen av Skogsstyrelsen (SKS) genomfört en uppföljande granskning av Skogsstyrelsens interna styrning och kontroll av informationssäkerhetsarbetet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa SKS:s uppmärksamhet på i denna revisionsrapport.

Riksrevisionen önskar information senast 2011-04-21 med anledning av våra iakttagelser i denna rapport.

Inledning

Riksrevisionen har i revisionsrapport daterad 2009-06-29 (dnr 32-2009-0595) framfört ett antal synpunkter på SKS:s arbete med informationssäkerhetsfrågor. Riksrevisionen bedömer efter genomförd uppföljning att SKS har genomfört flera viktiga åtgärder och beslut i arbetet med att införa ett ledningssystem för informationssäkerhet (LIS). Väsentliga styrdokument i ett LIS är fastställda av myndighetens chef. Riksrevisionen är medveten om att ett arbete med att införa LIS pågår, att prioriteringar varit nödvändiga och att viktiga åtgärder som ännu inte är genomförda enligt beslut är planerade att genomföras under 2011. Ansvar och roller för inblandade aktörer i arbetet med informationssäkerhet finns beskrivna och beslutade av GD. Det finns i och med beslut och framtagna styrdokument förutsättningar för en formaliserad struktur i det fortsatta arbetet med att införa och styra ett LIS.

Riksrevisionen bedömer dock att SKS interna styrning och kontroll av arbetet med informationssäkerhet ännu inte är fullt tillfredsställande och vill fästa SKS uppmärksamhet på nedanstående iakttagelser som främst berör drift- och supportenhetens arbete.

Drift- och supportenhetens arbete

Uppföljningen har precis som den tidigare granskningen visat att SKS har en låg grad av systematik i driften av servrar, nätverk etc. Rutinbeskrivningar för viktiga moment i driftarbetet saknas. Till exempel saknas rutinbeskrivningar för driftpersonalens hantering av säkerhetskopiering, återstart av servrar, återläsning och test av säkerhetskopior, skydd av källdata, loggning av privilegierade användares aktiviteter i operativsystem och databaser och uppföljningsaktiviteter inom drift- och supportenheten. SKS har bland annat angett kompetensstrukturen på drift- och supportenhetens personal som förklaring och att mycket arbete har behövt läggas på att centralisera IT-miljön. Trots rimliga förklaringar till orsakerna bakom iakttagna brister bedömer Riksrevisionen ändå bristerna som riskfyllda för informationssäkerheten på SKS.

I arbetet med att centralisera IT-miljön finns det flera faktorer som kan påverka informationssäkerheten negativt och som motiverar en högre grad av systematik redan i nuläget innan arbetet med en förflyttning påbörjas. I samband med fysisk och virtuell flytt av system och data kan det uppstå oplanerade avbrott och informationsförluster i olika omfattning, och i samband med en centralisering är det verksamhetskritiskt att personal med unika kunskaper och behörigheter finns tillgängliga och agerar utifrån fastställda rutiner. SKS bör i förebyggande syfte i riskanalysera kritiska moment och införa åtgärder för att minska riskerna till godtagbar nivå.

Med nuvarande grad av systematik i arbetet bedöms drift- och supportenhetens arbete som känsligt för nyckelpersonsberoende och att det finns betydande risker för ett ad hoc beteende, som kan leda till att uppgifter inte fullt ut utförs på tänkt sätt. Frånvaron av rutinbeskrivningar gör att Riksrevisionen bedömer att drift- och supportenhetens aktiviteter för att säkerställa en säker driftsmiljö inte är möjliga att följa upp på ett systemstiskt sätt.

Rekommendation

Riksrevisionen rekommenderar att SKS vidareutvecklar arbetet med framtagandet av beslutade och dokumenterade rutiner och riktlinjer för drift- och supportenhetens arbete. Vidare rekommenderas att utveckla arbetet med riskanalyser och påföljande skyddsåtgärder, i syfte att minska riskerna för störningar av stödet till verksamheten.

Systemförvaltningsmodell

SKS har beslutat om en modell för systemförvaltning. Modellen täcker bl.a. områden såsom formaliserat förfarande för acceptanstest och driftsättning, vilka Riksrevisionen tidigare haft synpunkter på.

I samband med utveckling och ändring av system finns det risker med att projektverksamheten blir en alltför dominant aktör i förhållande till beställande och mottagande verksamhet vid utveckling och ändring av system. Riksrevisionen bedömer därför att kravställande verksamhets

medverkan vid acceptanstest och godkännande innan driftsättning kan och bör lyftas fram.

Rekommendation

SKS bör vidta kompletterande åtgärder för att ytterligare förstärka arbetet med ledningssystem för informationssäkerhet (LIS) samt utveckling och ändring av system.

Ansvarig revisor Frank Lantz har beslutat i detta ärende. Uppdragsledare Lina Palmgren har varit föredragande. IT-revisor Mikael Pettersson har medverkat i den slutliga handläggningen.

Frank Lantz Lina Palmgren

Kopia för kännedom:

Regeringen