Sveriges Lantbruksuniversitet
Box 7070
750 07 UPPSALA

Datum 2010-02-08
Dnr 32-2009-0598

STYRNING AV INFORMATIONSSÄKERHETS-ARBETET VID SLU

Riksrevisionen har som ett led i den årliga revisionen av Sveriges Lantbruksuniversitet (SLU) granskat universitetets arbete med styrning och uppföljning av informationssäkerhetsfrågor.

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

Riksrevisionen önskar information senast 2010-05-10 med anledning av iakttagelserna i denna rapport.

1. Sammanfattning

Riksrevisionen har under hösten 2009 granskat hur SLU arbetar med styrning och uppföljning av informationssäkerhetsfrågor (fortsättningsvis i rapporten benämnt Ledningssystem för informationssäkerhet (LIS)), samt i vilken utsträckning detta arbete är integrerat med det generella arbetet med intern styrning och kontroll. Styrande regelverk som utgjort bedömningsgrund för iakttagelser och rekommendationer i rapporten är förordningen (2007:603) om intern styrning och kontroll (FISK) och förordningen (2003:770) om statliga myndigheters arbete med säkert elektroniskt informationsutbyte, med tillhörande föreskrifter. Granskningen har utförts genom intervjuer med IT-chefen, säkerhetschefen och universitetsdirektören samt genom dokumentstudier av styrande dokument för universitetets informationssäkerhetsarbete. Frågan har också berörts vid diskussioner med samordningsansvarig för universitetets arbete med intern styrning och kontroll.

Granskningen har visat att SLU har vissa delar av ett LIS på plats, men att flera viktiga komponenter som bör finnas i ett LIS för att säkra myndighetens interna kontroll och applikationernas tillförlitlighet, saknades vid granskningstillfället. I sammanhanget bör noteras att formerna för arbete med informationssäkerhetsfrågor har förändrats under 2009, dels då ansvaret för dessa frågor flyttats från IT-enheten till säkerhetsenheten, dels då tjänsten som informationssäkerhetssamordnare under hösten 2009 har varit vakant.

Den informationssäkerhetspolicy som gäller vid SLU beslutades 1997, och har enligt den information Riksrevisionen fått inte genomgått någon formell omprövning sedan dess. En väsentlig utgångspunkt i policyn är att särskilda säkerhetsanalyser, säkerhetshöjande åtgärder samt kontroller och uppföljningar ska göras för de system som myndighetens ledning bedömt

vara särskilt viktiga för verksamheten. Såvitt Riksrevisionen erfar finns dock inget beslut som pekar ut vilka system det är som anses vara särskilt viktiga, med följd att de i policyn beslutade åtgärderna inte heller tycks ha genomförts.

SLU:s ledning rekommenderas att ta ställning till hur informationssäkerhetsarbetet på myndigheten fortsättningsvis ska styras och utföras. För att förstärka den interna kontrollen i informationssäkerhetsarbetet rekommenderas att sträva mot en tydligare koppling mellan riskanalys, utformningen av kontrollåtgärder och uppföljning av dessa. För att den interna styrningen och kontrollen ska förbättras rekommenderas även att i en högre omfattning integrera arbetet med informationssäkerhet (LIS) och FISK.

2. Inledning

Utan en god informationssäkerhet finns det alltid risk att organisationens krav på riktighet, tillgänglighet och, i förekommande fall, sekretess rörande viktig information inte kan tillgodoses. Bristande informationssäkerhet har negativ påverkan på myndighetens interna styrning och kontroll liksom på myndighetens förmåga att lösa sina uppgifter på ett effektivt och säkert sätt. För att påvisa en god intern styrning och kontroll förutsätts därför att även en säker hantering av informationstillgångarna kan påvisas.

3. Normgivande regelverk

De normer som Riksrevisionen använt sig av vid bedömningen är

- Förordningen (2007:603) om intern styrning och kontroll (FISK).
- Myndighetsförordningen(2007:515).
- Förordning (2003:770) om statliga myndigheters arbete med säkert elektroniskt informationsutbyte.
- Verkets för förvaltningsutveckling (VERVA) tillämpningsföreskrifter (VERVAFS 2007:2) till ovan nämnd förordning
- Commitee of Sponsoring Organizations of the Treadway Commmission (COSO).

FISK definierar arbetet med intern styrning och kontroll som den process som syftar till att myndigheten med rimlig säkerhet fullgör de krav som framgår av tredje paragrafen i myndighetsförordningen.

Mot bakgrund av det ökande elektroniska informationsutbytet i samhället gav VERVA år 2007 ut en föreskrift som innebär att myndigheter under regeringen numera har explicita krav på sig att tillämpa ett systematiskt arbete med informationssäkerhet utifrån etablerad standard, ett så kallat ledningssystem för informationssäkerhet (LIS). Myndigheten VERVA är numera nedlagd, men de föreskrifter som gavs ut inom det aktuella området är fortfarande tillämpliga och skall efterlevas av samtliga myndigheter som

inte medgivits undantag av regeringen. I väsentliga delar utgör föreskrifterna, samt underliggande material till dessa, grund för de rekommendationer som lämnas i denna rapport.

För att beskriva intern styrning och kontroll har den så kallade COSO-modellen blivit ett vedertaget begrepp. FISK bygger sin struktur på COSO som beskriver intern styrning och kontroll i olika komponenter och deras inbördes samband. Komponenterna i COSO är kontrollmiljö, riskanalys, kontrollåtgärder, information/kommunikation och uppföljning. Kapitel 4 i denna rapport är indelat utifrån COSO-komponenterna med syfte att beskriva hur de olika iakttagelserna som gjorts avseende informationssäkerhetsarbetet kan återspeglas i ett större intern kontrollperspektiv.

4. Informationssäkerhet

4.1. Kontrollmiljö

Kontrollmiljön är grundförutsättningen för intern styrning och kontroll i organisationen och en förutsättning för de andra COSO-komponenternas funktionalitet. Kontrollmiljön återspeglas bl.a. i ledningens filosofi, attityder/inställning och ledarstil, hur den delar ansvar och befogenheter, organiserar och utvecklar medarbetare samt följer upp fattade beslut. En viktig komponent i kontrollmiljön är organisationskulturen då den påverkar medarbetares engagemang och medvetenhet.

SLU bedriver ett arbete med intern styrning och kontroll utifrån FISK-förordningen. Granskningen har dock visat att universitetets informationssäkerhetsarbete inte är integrerat i FISK-processen i någon vid bemärkelse, vilket det bör vara enligt Riksrevisionens uppfattning. För att ett LIS ska fungera på ett tillfredsställande sätt är det en nödvändighet att informationssäkerhet beaktas i den interna styr- och kontrollprocessen på ledningsnivå. Om inte informationssäkerhetsfrågor beaktas i arbetet med FISK finns det även risk att ledningens bedömning av den interna styrningen och kontrollen inte blir helt tillförlitlig.

I SLU:s informationssäkerhetspolicy anges att universitetsledningen är ytterst ansvarig för informationssäkerheten, men att prefekt eller motsvarande ansvarar för säkerheten inom sitt område. För att detta ansvar ska kunna tas krävs dock att utbildning, information samt lämpliga regelverk finns tillhanda för den person som fått ansvaret delegerat till sig. Riksrevisionen har vid granskningen inte kunnat se att utbildning eller information i dessa frågor ges till berörda personer på ett systematiskt sätt.

Ett grundläggande begrepp avseende informationssäkerhetsarbetet är att det bör finnas en utsedd system- eller informationsägare för varje system/applikation myndigheten har. Vid förfrågan har någon samlad förteckning över vem som äger de olika systemen inom SLU inte kunnat erhållas. Detta medför att revisionen inte har kunnat erhålla någon överblicksbild över om alla informationsresurser och system verkligen har en utsedd ansvarig. Frågan försvåras något av den decentraliserade

organisationen vid SLU, där IT-enheten inte handhar driften av alla system utan institutionerna själva kan välja andra driftsalternativ för vissa system. En sådan organisation kan i vissa lägen vara mera kostnadseffektiv, men ökar också kraven på formella rutiner för överblick av vilka informationsmängder och applikationer som finns inom myndigheten.

Det decentraliserade ansvaret ställer särskilda krav på tydlighet i policy och riktlinjer för informationssäkerhetsarbetet. Ledningen har alltid ansvaret för myndighetens informationssäkerhet och en policy ska därför uttrycka ledningens syn på behovet av, och mål för informationssäkerheten. Vid SLU finns en informationssäkerhetspolicy daterad 1997. Vid granskningen har inte framkommit information om huruvida denna underställts formell, regelbunden prövning med avseende på innehåll mm, något som bör göras. Informationssäkerhetspolicyn bör vidare kompletteras med mera operativa riktlinjer och regelverk. Vid granskningen har vissa sådana riktlinjer identifierats, men för flera viktiga områden, såsom distansarbete och hantering av externa lagringsmedia (USB-minnen mm) har denna typ av dokument inte kunnat identifieras. Oklarheter om vilka regler och rutiner som gäller i dessa frågor ökar risken att viktig information går förlorad, eller sprids på ett icke avsett sätt.

Rekommendation

SLU bör vidta åtgärder för att öka styrning och samordning av informationssäkerhetsarbetet, samt bedöma i vilken grad detta bör interagera med myndighetens arbete enligt förordningen om intern styrning och kontroll. Vidare bör SLU införa en rutin för regelbunden, dokumenterad omprövning av innehåll och inriktning i informationssäkerhetspolicyn, samt tillse att kompletterande regler och riktlinjer för informationssäkerhetsområdet utarbetas, baserat på myndighetens bedömning av viktiga/riskfyllda delområden.

4.2. Riskanalys

I riskanalysarbetet är organisationens mål och uppdrag den primära utgångspunkten. I riskanalysen ingår att identifiera, värdera och aktivt ta ställning till hur risker ska hanteras, d v s om de ska elimineras, reduceras eller accepteras. Riskanalysen är grundläggande för att utforma handlingsplaner och kontrollåtgärder i syfte att minska riskerna till en godtagbar nivå. Riskanalys bör genomföras på samtliga organisatoriska nivåer.

Utgångspunkter för att en riskanalys inom informationssäkerhetsområdet ska kunna genomföras på ett adekvat sätt är dels att det finns en tydlig bild av vilka system och informationsmängder verksamheten innehar, dels att man genom en informationsklassning skapat en samlad bild över vilken känslighet respektive informationsmängd/system har för störningar avseende tillgänglighet, sekretesskrav samt integritet/riktighet i informationsinnehållet. Någon formell process/rutinbeskrivning för informationsklassning finns idag inte vid SLU, och Riksrevisionen har inte heller funnit någon samlad

överblick över vilka system och informationsmängder myndigheten totalt har.

En grundläggande punkt i SLU:s informationssäkerhetspolicy är att ett antal särskilda moment avseende bl.a. särskilda riskanalyser, uppföljningsrutiner och kontrollåtgärder ska genomföras för de system som är "viktiga för verksamheten". Något ledningsbeslut om vilka system som anses uppfylla detta kriterium har dock inte kunnat identifieras, och därmed har ett antal av de i policyn beslutade åtgärderna inte heller kunnat verifieras, och troligen inte heller genomförts.

Av den dokumentation Riksrevisionen tagit del av framgår inte tydligt vilka befattningshavare inom organisationen som ansvarar för att riskanalyser avseende informationssäkerheten ska genomföras. En rimlig tolkning är dock att detta ligger i det delegerade ansvaret till verksamhetsansvariga i informationssäkerhetspolicyn. Detta kräver dock att stöd tillhandahålls avseende metodik för genomförande av dessa analyser, vägledning i hur risker ska värderas och i ett senare skede kunna reduceras/elimineras. Något myndighetsgemensamt beslutat stöd av denna typ har inte kunnat identifieras vid granskningen. Dock har noterats att viss dokumentation har utarbetats internt inom säkerhetsenheten, med denna inriktning.

Av informationssäkerhetspolicyn framgår vidare att skyddsåtgärder för respektive system ska införas utifrån en särskild säkerhetsanalys, och det ska också genomföras riskanalyser innan ett nytt system införs i verksamheten eller förändring görs av ett befintligt system. Någon samlad uppföljning av att dessa moment i policyn efterlevs har inte kunnat identifieras vid granskningen.

Rekommendation

Den beslutade informationssäkerhetspolicyn utgår alltså i mångt och mycket från att SLU:s ledning har fastställt vilka system som ska anses vara viktiga för verksamhetens genomförande; ett beslut inte kunnat identifieras vid granskningen. SLU bör därför inlednings verka för en ökad samlad överblick över vilka större system och informationsmängder myndigheten totalt har. Därefter bör en strukturerad informationsklassning av berörda system och informationsmängder genomföras för att bedöma väsentligheten för verksamheten. Denna information bör sedan ligga till grund för riskanalysarbetet. SLU bör också eftersträva att införa och tillhandahåll en riskanalysmodell som kan användas generellt i verksamheten av de personer som tilldelats ansvaret att genomföra riskanalyser.

4.3. Kontrollåtgärder

Ledningen ska utifrån resultatet av riskanalysen ta ställning till hur riskerna ska hanteras. Kontrollåtgärderna ska motverka identifierade risker, vara inbyggda i organisationens processer/rutiner och kan vara både manuella och automatiska (programmerade kontroller). Ytterst ska kontrollåtgärderna bidra till att myndigheten når sitt mål och att ledningens direktiv för verksamheten genomförs. Kontrollåtgärder kan ske på alla nivåer i organisationen.

I SLU:s informationssäkerhetspolicy läggs ett antal olika kontrollåtgärder fast avseende bl.a. rapportering av incidenter till IT-säkerhetsenheten, rutiner för arkivering och genomgång av systemloggar, säkerhetskrav i avtal med externa parter mm. På andra viktiga områden såsom behörighetshantering har någon central policy/riktlinje dock inte kunnat identifieras. Generellt tycks gälla att de rutinbeskrivningar mm som identifierats vid granskningen tillämpas inom och av IT-enheten för de resurser där man har driftsansvaret, men det är svårt att få någon bild av tillämpningen för övriga applikationer och system vilka inte hanteras inom IT-enhetens ram. Ur ett intern kontrollperspektiv är det viktigt att myndighetsledningen säkerställer en enhetlig syn på och hantering av informationssäkerhetsfrågor oavsett vem som har det operativa ansvaret för driften. Någon sådan samlad överblick och styrning inom SLU har inte kunnat identifieras vid granskningen.

Rekommendation

För att uppnå en lämplig intern kontrollnivå bör SLU utveckla arbetet med att tillhandahålla centrala riktlinjer och regelverk för informationssäkerhetsfrågor. Oavsett vilken form som de delegerade enheterna inom myndigheten väljer för drift, support mm bör det finnas ett antal central fastställda rutiner och kontroller som tillämpas generellt i verksamheten. Dessa kan sedan med fördel kompletteras med lokalt beslutade regler, riktlinjer och kontrollfunktioner utifrån den lokalt identifierade riskbilden.

4.4. Information och kommunikation

En förutsättning för intern styrning och kontroll är att ledningen ger ett tydligt budskap avseende exempelvis mål, risker, ansvar, befogenheter, rutiner och instruktioner. Ansvariga måste förstå sin egen roll avseende informationssäkerhet och hur enskilda aktiviteter påverkar andra aktiviteter. Ledningen måste säkerställa att kommunikation når fram och att information inte fastnar på vägen. Behovet av tydlighet och kommunikation är särskilt stort i organisationer där verksamheter är geografiskt.

Enligt SLU:s informationssäkerhetspolicy skall personalen informeras och utbildas i informationssäkerhetsfrågor. Vid granskningen har inte kunnat identifieras någon process som säkerställer att detta sker med lämplig regelbundenhet.

Rekommendation

SLU rekommenderas att se över hur informationssäkerhetspolicyns nuvarande krav på information och utbildning till anställda och andra systemanvändare avseende informationssäkerhetsfrågor.

4.5. Uppföljning

Uppföljning behöver genomföras på alla ledningsnivåer för att säkerställa måluppfyllelse och att risker hanterats enligt beslut. Omfattningen och

frekvensen beror i första hand på värderingen av identifierade risker och verksamhetens komplexitet. Ledningen är ansvariga för uppföljning och utvärdering av verksamhetens interna styr- och kontrollsystem. Med avseende på informationssäkerhet är beslutad policy och riktlinjer de av ledningen fastställda kriterier mot vilka intern styrning och kontroll kan följas upp.

Av VERVAFS 2007:2 framgår det att samordnaren för informationssäkerhet ska redovisa en åtgärdsplan (handlingsplan) inklusive uppföljning för myndighetens ledning. Ett motsvarande krav står också inskrivet i SLU:s informationssäkerhetspolicy, och en sådan skriftlig rapportering har också gjorts till universitetsdirektören. Därutöver går också månadsrapportering avseende incidenter mm till IT-chef och säkerhetschef. Det framgår dock inte av beslut eller liknande vilka åtgärder, om några, som vidtagits med anledning av den rapportering som gjorts från informationssäkerhetssamordnaren.

Enligt informationssäkerhetspolicyn skall de system som SLU bedömt vara viktiga för verksamheten ha en plan för återkommande uppföljning och kontroll. Säkerhetsanalys skall genomföras vart tredje år och särskilda rutiner ska inrättas för att följa upp de iakttagelser som gjorts. Vidare skall en aktiv uppföljning göras av att berörda systemägare efterlevt dessa krav och informationen enligt ovan skall tjäna som input till kommande säkerhetsanalyser. Som konstateras ovan har det vid granskningen inte kunnat identifieras något beslut om vilka system som är "viktiga" och därmed ska omfattas att dessa regelverk. Ledningen har därmed inte heller kunnat erhålla information utifrån dessa parametrar.

Rekommendation

SLU bör till se att särskild uppföljning av informationssäkerhetsarbetet görs utifrån de parametrar som idag finns beslutade i informationssäkerhetspolicyn, alternativt utifrån en ny prioritering i en omprövad policy. SLU bör vidare överväga de framtida formerna för rapportering till ledningen av denna typ av frågor, mot bakgrund av de rekommendationer och krav som ges i VERVAFS 2007:2.

Ansvarig revisor Frank Lantz har beslutat i detta ärende. Uppdragsledare Dan Pederson har varit föredragande.

Frank Lantz

Dan Pederson

Kopia för kännedom:

Regeringen