Revisionsrapport

RIKSREVISIONEN

Linköpings universitet
581 83 Linköping

Datum 2010-01-19
Dnr 32-2009-0643

Granskning av intern styrning och kontroll av informationssäkerheten vid Linköpings universitet 2009

Riksrevisionen har som ett led i den årliga revisionen granskat Linköpings universitets (LiU) interna styrning och kontroll av informationssäkerhet.

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

Riksrevisionen önskar information senast 2010-03-08 med anledning av våra iakttagelser i denna rapport.

Sammanfattning

Mot bakgrund av det ökande elektroniska informationsutbytet i samhället har myndigheter under regeringen numera explicita krav på sig att tillämpa ett systematiskt arbete med informationssäkerhet utifrån etablerad standard, ett så kallat ledningssystem för informationssäkerhet (LIS).

Riksrevisionen har under 2009 granskat hur LiU arbetar med ett LIS och i vilken utsträckning detta arbete är integrerat med myndighetens interna styrning och kontroll.

Riksrevisionen bedömer att vissa åtgärder vidtagits på ledningsnivå men att åtgärderna inte är tillräckliga och att de inte kommunicerats och implementerats i verksamheten fullt ut. Granskningen har visat att förbättringar behövs på en rad områden för att ledningssystemet för informationssäkerhet ska motsvara etablerad standard.

Information är en av de viktigaste tillgångarna vid en myndighet. Oavsett vilken form informationen har, på vilket sätt den överförs eller lagras, ska den få tillräckligt skydd. Brister i informationssäkerheten medför att tillförlitligheten i myndighetens interna kontroll försvagas och att det finns risker för informationens riktighet, sekretess, tillgänglighet och spårbarhet. Intern styrning och kontroll förutsätter därför att en god informationssäkerhet och säker hantering av informationstillgångarna kan visas.

Riksrevisionens granskning visar att det finns ett ramverk för styrning av informationssäkerheten i form av en informationssäkerhetspolicy för LiU men att de fastställda riktlinjer som finns inom området inte är tillräckliga utifrån etablerad standard. Kunskapen om policyn och dess innehåll är inte

tillräcklig bland ansvariga för att kunna styra arbetet med informationssäkerhet.

LiU har inte genomfört riskanalyser för informationssäkerhet på universitetsövergripande nivå. Därför saknas också en sammanställd bild över vilka risker som bör prioriteras vid LiU. Det var vid granskningstillfället inte tydligt hur informationssäkerhetsrisker tas om hand i de riskanalyser som genomförs inom ramen för förordning om intern styrning och kontroll (FISK).

Det saknas i stor utsträckning dokumenterade kontrollåtgärder för informationssäkerheten.

Granskningen visar också att rutiner saknas för uppföljning inom området och att uppföljning varken genomförts av samordningsansvarig eller universitetets styrelse/ledning.

För att universitetets styrelse/ledning ska ha ett relevant och tillförlitligt underlag vid bedömning av den interna styrningen och kontrollen behöver arbetet med LIS integreras i arbetet enligt förordningen om intern styrning och kontroll (FISK) i en högre utsträckning.

1. Inledning

Intern styrning och kontroll förutsätter en god informationssäkerhet. Utan god informationssäkerhet finns det betydande risker för informationens riktighet, sekretess, tillgänglighet och spårbarhet. Bristande informationssäkerhet har negativ påverkan på myndigheters interna styrning och kontroll och vice versa. Informationssäkerhet och intern styrning och kontroll står därmed i ett ömsesidigt beroende till varandra. Brister i ledningens upprättande och genomförande av generella kontroller för att uppnå en god informationssäkerhet kan medföra att myndighetens interna styrning och kontroll försvagas. För att påvisa en god intern styrning och kontroll förutsätts också en säker hantering av informationstillgångarna.

2. Normgivande regelverk

De normer som Riksrevisionen använt sig av vid bedömningen är

- Förordning (2007:603) om intern styrning och kontroll (FISK),
- Myndighetsförordning (2007:515),
- Högskoleförordning (2003:100),
- Förordning (2003:770) om statliga myndigheters arbete med säkert elektroniskt informationsutbyte,

- Vervas föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2),
- Vervas allmänna råd till föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2),
- Commitee of Sponsoring Organizations of the Treadway Commission (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 3§ i myndighetsförordningen. Vidare framgår det av 2§ i högskoleförordningen att det är styrelsens ansvar att säkerställa att det vid universitetet finns en intern styrning och kontroll som fungerar på ett betryggande sätt.

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.

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. Det innebär att myndigheten ska upprätta en policy för informationssäkerhet och andra styrande dokument som behövs för myndighetens informationssäkerhet.

Begreppet informationssäkerhet är ett vidare begrepp än IT-säkerhet och fokuserar på informationens säkerhet snarare än IT-systemens säkerhet. Information förekommer i många former och oavsett vilken form den har, på vilket sätt den överförs eller lagras, måste den alltid ha ett godtagbart skydd.

3. Informationssäkerhet

3.1. Kontrollmiljö

Kontrollmiljön är grunden för intern styrning och kontroll i en organisation och de andra COSO-komponenternas förutsättning. Den återspeglas bl. a. i ledningens filosofi, attityder/inställning och ledarstil, hur ledningen 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.

Riksrevisionens granskning har visat att det vid LiU finns ett ramverk i form av beslutad policy, förvaltningsmodell och vissa riktlinjer för informationssäkerhet. Riktlinjerna finns i form av bilagor till policyn. Fler universitetsgemensamma riktlinjer behövs dock för att ramverket ska

återspegla etablerade standarder inom området. Väsentliga riktlinjer som bör finnas i ett LIS saknas, t.ex. riktlinjer för hantering av behörigheter, informationsklassning, incidenthantering, skalskydd för datahallar och loggning (spårbarhet).

Det finns regler för administratörer, användare och studenter för användning av dator-, nät- och systemresurser vid LiU. Dessa regler bör fastställas som universitetsgemensamma riktlinjer på policynivå för att understryka vikten av dessa regler och dess efterlevnad. Det bör från ledningsnivå tydligt visas vad som förväntas av anställda när det gäller internetanvändning, etik, etc. Det bör också framgå att all e-posttrafik loggas som ett led i säkerhetsarbetet.

Policyn är tydlig gällande beskrivningen av ansvar och roller. Även LiUs förvaltningsmodell beskriver ansvaret för systemägare. Granskningen har dock visat att systemägaransvaret och definitionen av de olika rollerna inte fullt ut är kända i organisationen. Kunskapen om det egna ansvaret på institutionsnivå varierar men bedöms vara låg hos majoriteten av de intervjuade. En trolig orsak är att policyn inte har kommunicerats ut från ledning till övriga verksamheter i tillräcklig utsträckning.

Ledningen har inte i tillräcklig utsträckning kunskap om vilka informationstillgångar som finns ute på institutions-, avdelningsnivå, var informationen finns och vilket skyddsvärde den har. Detta är sannolikt en följd av att det saknas riktlinjer för informationsklassning och att det inte finns någon tradition av att genomföra sådana klassningar. Det framgår även av LiUs förvaltningsmodell att säkerhetsnivån ska fastställas vilket förutsätter en klassning av informationen. Utan klassning går det inte att med rimlig säkerhet bedöma informationens skyddsvärde och vilka åtgärder som behöver vidtas för att undvika negativa konsekvenser för universitetet. Vid granskningstillfället har det inte gått att få fram någon aktuell dokumentation som anger vilka som är systemägare och förvaltare för system på institutionsnivå.

Riksrevisionen *rekommenderar* LiU att fastställa riktlinjer för att i större utsträckning få ett komplett ramverk för informationssäkerhet som motsvarar etablerad standard inom området.

Riksrevisionen *rekommenderar* LiU att fastställa rutiner för information till och utbildning av olika användarkategorier om ansvar, policy och riktlinjer för informationssäkerhet.

3.2. Riskanalys

I riskanalysarbetet är organisationens mål och uppdrag den primära utgångspunkten. Riskanalysen är grunden för att utforma en lämplig åtgärdsplan och kontrollåtgärder i syfte att minska riskerna till en godtagbar nivå. Riskanalys bör genomföras på samtliga organisatoriska nivåer.

Utgångspunkten för informationssäkerhetsarbetet är att riskanalyser genomförs för att kartlägga den säkerhetsnivå som ska gälla för skydd av

informationen. Ur ett informationssäkerhetsperspektiv är informationsklassning, rapporterade incidenter och uppföljningar viktiga informationskällor för att upprätta en bra riskanalys. Ett effektivt riskanalysarbete förutsätter kunskaper från både kärnverksamhet och IT-, informationssäkerhetsområdet.

Om informationssäkerhetsfrågor inte full ut beaktas i arbetet med FISK finns risk för att styrelsens/ledningens underlag för bedömning av den interna styrningen och kontrollen inte är tillförlitligt.

LiU har inte genomfört någon riskanalys för informationssäkerhet på universitetsövergripande nivå. Vervas tillämpningsföreskrift föreskriver att en myndighet utifrån risk- och sårbarhetsanalyser och dokumenterade incidenter ska avgöra vilka risker som ska elimineras, reduceras eller accepteras, samt besluta om åtgärder för myndighetens informationssäkerhet. Informationssäkerhet har i viss utsträckning beaktats i samband med riskanalysen i FISK-arbetet. Vid granskningstillfället framkom att den riskanalys som gjorts i samband med FISK-arbetet övergripande beaktat endast en risk relaterad till informationssäkerhet. Bland ansvariga för informationssäkerhet rådde det osäkerhet kring hur och varför just denna risk lyfts. Senare gavs information från annat håll i organisationen om att det identifierats fler risker med bäring på informationssäkerhet. Detta indikerar att personer med ansvar för och kunskap om informationssäkerhet inte i tillräcklig utsträckning varit involverade i den genomförda riskanalysen (FISK).

Hälften av de institutioner som besöktes i samband med granskningen har egna servrar, databaser som är placerade både fysiskt och virtuellt på institutionerna. Riskmedvetenheten och kunskapen om informationens skyddsvärde varierar. Endast en av de besökta institutionerna hade vid granskningstillfället genomfört en formaliserad riskanalys. Ingen av institutionerna hade genomfört klassning för att bedöma vilket skyddsvärde informationstillgångarna har. Vid granskningstillfället uppgav ansvariga för informationssäkerheten att det inte genomförts några dokumenterade riskanalyser eller informationsklassningar för de gemensamma administrativa systemen.

Riksrevisionen *rekommenderar* LiU att genomföra en riskanalys för informationssäkerhet samt besluta om hur identifierade risker ska hanteras. Riskanalysen bör ha sin grund i riskanalyser genomförda på lägre nivåer inom LiU samt riskanalyser för specifika system. LiU bör ta ställning till hur detta arbete ska integreras i det riskanalysarbete som pågår inom ramen för FISK.

LiU bör beakta informationens skyddsvärde med hjälp av klassningar, rapporterade incidenter och uppföljningar. Personer med ansvar och kunskap avseende informationssäkerhet bör i högre utsträckning involveras i arbetet med riskanalys.

3.3. Kontrollåtgärder

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

Riksrevisionens granskning har visat att förekomsten av dokumenterade kontrollåtgärder är låg. Dokumenterade rutinbeskrivningar som är viktiga för kontroll och styrning av informationssäkerhet saknas i stor utsträckning.

Rutiner för behörigheter är en förutsättning för ett systematiskt arbete med att tilldela, ändra, ta bort och följa upp behörigheter. Granskningen har visat att dokumenterade rutiner för hantering av behörigheter saknas på såväl institutionsnivå som central nivå. Dokumenterade rutiner för hantering av privilegierade behörigheter för databaser, operativsystem mm saknas. Det görs ingen regelbunden eller dokumenterad uppföljning av privilegierade behörigheter, vilket är förenat med risker för hela myndigheten.

Riksrevisionen har fått information om att det finns en kontinuitets-/avbrottsplan för den centrala driften. Granskningen visade dock att LiU saknar dokumenterade och fastställda kontinuitets-/avbrottsplaner för de gemensamma administrativa systemen som anger återställningstider, reservplaner vid avbrott, rutiner för återstart, krav på säkerhetskopiering, återläsningstester etc.

Enligt information från ansvariga ska kontinuitets-/avbrottsrelaterad information återfinnas i förvaltningsplanerna för respektive system. De två förvaltningsplaner som Riksrevisionen tagit del av omfattar dock inte innehållet i en kontinuitets-/avbrottsplan.

Förvaltningsplaner har bland annat som syfte att åstadkomma en systematisk plan för förvaltning av de olika systemen. Aktuella förvaltningsplaner som följer en beslutad modell är en förutsättning för att åstadkomma en systematisk förvaltning. LiU har en beslutad modell för förvaltning av systemen och har även tagit fram en mall för framtagande av förvaltningsplaner. Riksrevisionen har begärt att få del av förvaltningsplaner för fem viktiga gemensamma administrativa system men har endast erhållit två. LiU har inte kunnat visa att det finns förvaltningsplaner för övriga. Ingen av de två förvaltningsplanerna som erhållits beskriver några säkerhetsåtgärder. Dessa planer var inte heller kompletta i jämförelse med den av LiU beslutade mallen. Förvaltningsplaner fanns inte heller vid någon av de besökta institutionerna som uppgett att de har system med viktig information.

Riksrevisionen bedömer att LiUs beslut om förvaltningsmodell inte efterlevs för viktiga administrativa system eller av de institutioner som omfattades av granskningen. Ansvariga för informationssäkerheten har inte tillräcklig kunskap om förvaltningsplaners förekomst, aktualitet och innehåll.

Granskningen visade också att det på institutionsnivå inte finns några dokumenterade rutiner för att säkerställa att säkerhetskopior tas, att dessa har en skyddad förvaring och återläsningstestas regelbundet.

Riksrevisionen *rekommenderar* LiU att, med riskanalyser som grund, på ett mer systematiskt sätt arbeta med dokumenterade kontrollåtgärder för att motverka identifierade risker inom informationssäkerhetsområdet. Rutiner för behörighetshantering, kontinuitetsplanering samt rutiner som säkerställer säkerhetskopiering, återläsningstester och att materialet skyddas från yttre påverkan bör fastställas.

Riksrevisionen *rekommenderar* LiU att upprätta förvaltningsplaner för samtliga system och att dessa följer LiUs beslutade förvaltningsmodell.

3.4. Information och kommunikation

En förutsättning för intern styrning och kontroll är att ledningen ger ett tydligt budskap om mål, risker, ansvar, befogenheter och rutiner.

Ledningen uppfattar att information om ansvar, roller och arbetsuppgifter är kommunicerade ut i verksamheten. Riksrevisionens granskning visar dock att verksamheten i flera fall inte i tillräcklig omfattning tagit del av information om informationssäkerhet.

Riksrevisionen lämnar rekommendationer avseende information och kommunikation under stycke 3.1 Kontrollmiljö.

3.5. Uppföljning

Uppföljning bör genomföras på alla ledningsnivåer för att säkerställa måluppfyllelse och att risker hanterats enligt beslut. Omfattning och frekvens beror på värderingen av identifierade risker och verksamhetens komplexitet. Styrelse/ledning är ansvariga för uppföljning och utvärdering av verksamhetens interna styr- och kontrollsystem. För informationssäkerhet är beslutad policy och riktlinjer ledningens fastställda kriterier mot vilka intern styrning och kontroll följs upp.

I anslutning till att årsredovisningen skrivs under ska också styrelsen lämna en bedömning av huruvida den interna styrningen och kontrollen varit betryggande under året. Om informationssäkerhetsfrågor inte fullt ut beaktas i arbetet med FISK finns risk för att ledningens underlag för bedömningen av den interna styrningen och kontrollen inte är tillförlitligt.

Av Vervas tillämpningsföreskrift framgår att det ska finnas en utsedd person som ansvarar för arbetet med informationssäkerhet och som minst en gång per år för myndighetsledningen redovisar och dokumenterar vilka granskningar och åtgärder av större betydelse som har vidtagits enligt

myndighetens policy och styrdokument. Vid LiU finns en utsedd person som ansvarar för samordning av arbetet med informationssäkerhet. Någon plan för granskningar och åtgärder fanns inte vid granskningstillfället och det har inte heller framkommit att någon sådan dokumentation finns.

Riksrevisionens granskning visar att det inte förekommer några systematiska uppföljningar av informationssäkerheten varken från ledningsnivå eller på institutionsnivå. Ingen av de intervjuade har genomfört någon dokumenterad uppföljning.

Riksrevisionen *rekommenderar* LiU att på ett systematiskt sätt, utifrån genomförda riskanalyser och kontrollåtgärder, följa upp informationssäkerheten. En sammanställd redovisning av genomförda uppföljningar bör redovisas till styrelsen, som i anslutning till underskriften i årsredovisningen ska lämna en bedömning av huruvida den interna styrningen och kontrollen är betryggande.

Ansvarig revisor Christina Fröderberg har beslutat i detta ärende. Uppdragsledare Mariette Hagenfjärd har varit föredragande. IT-revisor Mikael Pettersson har medverkat i den slutliga handläggningen.

Christina Fröderberg

Mariette Hagenfjärd

Kopia för kännedom:

Regeringen

Internrevisionen, Linköpings universitet