Lunds universitet
Box 117
221 00 LUND

Datum 2010-01-22
Dnr 32-2009-0644

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

Riksrevisionen har som ett led i den årliga revisionen granskat den interna styrningen och kontrollen av informationssäkerheten vid Lunds universitet (LU).

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

Riksrevisionen önskar information senast 2010-03-08 med anledning av iakttagelserna 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 LU arbetar med ett LIS och i vilken utsträckning detta arbete är integrerat med myndighetens interna styrning och kontroll.

Riksrevisionen bedömer att det finns brister i ledningens styrning och uppföljning av informationssäkerheten på LU och att detta har funnits i flera år. Granskningen visar 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, och 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.

LU har påbörjat en universitetsövergripande process med att upprätta ett LIS, men saknar i dagsläget ett beslutat ramverk som reglerar styrning och uppföljning av informationssäkerheten. Det finns dessutom oklarheter i ansvars-styrnings- och uppföljningsfrågor för informationssäkerheten. LU saknar en formellt utsedd person med samordningsansvar för arbetet med informationssäkerhet, och det genomförs inte några systematiska uppföljningar av

informationssäkerheten på LU. Det är inte heller tydligt var i organisationen ansvaret för uppföljning ligger.

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

LU rekommenderas bland annat att prioritera arbetet med att ta fram och fastställa universitetsgemensamma riktlinjer och praktiska anvisningar för informationssäkerhet, att tydliggöra ansvar och roller i arbetet samt att öka graden av systematik i arbetet med LIS. För att styrelsen ska ha ett relevant och tillförlitligt underlag vid bedömning om den interna styrningen och kontrollen behöver arbetet med LIS integreras i arbetet med FISK.

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 därför även att en säker hantering av informationstillgångarna kan garanteras.

2. Normgivande regelverk

De normer som Riksrevisionen har 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 säker 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 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 3§ myndighetsförordningen. Vidare framgår det av 2§ högskole-

förordningen 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 Verket för förvaltningsutveckling (Verva) 2007 ut en föreskrift som innebär att myndigheter under regeringen 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 och 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 bland annat i ledningens filosofi, attityd och ledarstil samt hur ledningen delar ansvar och befogenheter, organiserar och utvecklar medarbetare och följer upp fattade beslut. En viktig komponent i kontrollmiljön är organisationskulturen eftersom den påverkar medarbetares engagemang och medvetenhet.

Riksrevisionens granskning visar att LU saknar ett fastställt och universitetsgemensamt ramverk som reglerar styrning och uppföljning av informationssäkerheten, dvs. ett ledningssystem för informationssäkerhet (LIS). Denna iakttagelse har även tidigare rapporterats till LU.[1] Det pågår arbete med att ta fram en universitetsövergripande säkerhetspolicy samt riktlinjer och praktiska anvisningar för informationssäkerhet, men dessa var inte beslutade vid granskningstillfället.[2]

2003 beslutade rektor om föreskrifter för IT-säkerhet vid LU.[3] Granskningen visar att dessa inte har implementerats på ett tillräckligt sätt i organisationen och att de därför i stor utsträckning inte följs. Institutionerna upplever i flera fall föreskrifterna som otydliga. Det har inte tagits fram några metodanvisningar eller mallar som komplement till föreskrifterna.

---

[1] Revisions-PM 2008-04-01, dnr 32-2007-0743.

[2] Säkerhetspolicyn har senare beslutats av styrelsen 2009-09-26, dnr LS 2009/448.

[3] Föreskrifter för IT-säkerhet vid Lunds universitet, 2003-05-15, dnr I D 9 2189/2003.

Under 2003 granskade internrevisionen IT-säkerheten på institutionsnivå med föreskrifterna som utgångspunkt.[4] Den sammanfattande bedömningen var då att informationssäkerheten på institutionerna hade många brister och att säkerhetsnivån därmed inte kunde anses som tillräcklig. LU:s förslag på åtgärder med anledning av internrevisionens rapport var bland annat att inleda ett arbete med att ta fram ett LIS. Det är Riksrevisionens bedömning att man på de sex år som gått inte har lyckats slutföra ett sådant arbete.

Av Vervas föreskrifter framgår att det ska finnas en person som särskilt arbetar med samordning av informationssäkerheten samt årligen redovisar en åtgärdsplan inklusive uppföljning för myndighetens ledning. Någon sådan person finns i dag inte på LU. Granskningen har visat att ansvaret för samordning av informationssäkerheten på LU är oklart och att man inte vet var i organisationen en sådan person bör vara placerad. Som en följd av detta har LU inte kunnat påvisa en åtgärdsplan för informationssäkerhet inklusive beskrivna uppföljningsaktiviteter för ledningen på LU. Detta har inte heller efterfrågats av ledningen.

Återkommande iakttagelser från Riksrevisionens granskning är oklarheter i ansvar för informationssäkerheten. Detta gäller bland annat prefekters och systemägares ansvarsfördelning och har sin grund i LU:s decentraliserade och delvis komplexa organisation. Som exempel kan nämnas Ladok, där systemägaren är ansvarig för säkerheten i systemet medan prefekterna är ansvariga för säkerheten på institutionsnivå där Ladok i huvudsak används.

Granskningen visar även på otydligheter i ansvarsfördelningen mellan systemägare och Lunds Datacentral (LDC) samt kring vem som är ägare av informationen, elektronisk och annan, som finns inom LU. Enligt uppgift följer informationsägarskapet med systemägarskapet, men detta finns inte uttryckt i något beslutat dokument. Granskningen visar också att denna uppfattning inte är kommunicerad till alla berörda inom LU. Det finns inte formellt utsedda systemägare för samtliga system och det saknas rutiner som säkerställer att systemägare utses på institutioner eller motsvarande. Det finns i dag inte någon beslutad modell för systemförvaltning inom LU, men en sådan håller på att tas fram.

Riksrevisionen *rekommenderar* LU att prioritera arbetet med att ta fram och fastställa universitetsgemensamma riktlinjer och anvisningar för informationssäkerhet, samt att besluta om en samordnare för arbetet med informationssäkerhet. För detta arbete bör det finnas en beslutad tidplan.

Riksrevisionen *rekommenderar* LU att fastställa en modell för systemförvaltning samt fastställa och klargöra ansvar och befogenheter för system- och informationsägare, särskilt för system som används på flera nivåer och bredder inom organisationen.

---

[4] Årsrapport från Internrevisionen år 2003, 2004-02-06, dnr I B 6 690/2004 samt IT-revisionsrapport Institutionsgranskning, 2004-01-29 (Ernst & Young).

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 för informationssäkerhet förutsätter att kunskaper från både kärnverksamheten och IT-/informationssäkerhetsområdet integreras.

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

Av Vervas föreskrifter framgår 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.

LU har inte genomfört någon riskanalys för informationssäkerhet på universitetsövergripande nivå. Inte heller på lägre nivåer i organisationen har riskanalyser med fokus på informationssäkerhet utförts. Därför saknas en sammanställd bild över vilka risker och åtgärder inom informationssäkerhetsområdet som bör prioriteras vid LU.

Enligt LU:s föreskrifter för IT-säkerhet ska en säkerhetsplan upprättas för varje dator, datorsystem och funktion eller utrustning i kommunikationsnät där det är av vikt att driften inte störs. I säkerhetsplanen ska det bland annat finnas en riskanalys. Granskningen visar att sådana säkerhetsplaner, med vissa undantag, inte har upprättats inom LU. Säkerhetsplaner har heller inte efterfrågats av ledningen.

LU saknar i dag rutiner som säkerställer att riskanalyser görs på systemnivå. I tidigare granskningar har Riksrevisionen och Internrevisionen rapporterat att riskanalyser saknades för Ladok och fakturahanteringssystemet Lupin.[5] I den nu genomförda granskningen kan konstateras att riskanalys fortfarande inte finns för Ladok.

LU genomför riskanalyser för försäkringsbara risker enligt förordning (1995:1300) om statliga myndigheters riskhantering samt riskanalyser enligt FISK. Det var vid granskningstillfället inte tydligt hur dessa riskanalyser förhåller sig till informationssäkerhetsrelaterade risker och de riskanalyser som enligt regelverket bör genomföras specifikt för informationssäkerhet.

På LU saknas formella krav för informationsklassning. Det finns inte heller beslut om vilka system som är verksamhetskritiska. På institutionsnivå är det i vissa fall oklart vilka informationstillgångar som institutionerna

[5] Revisionspromemoria 2008-04-14, dnr 32-2007-0743 samt Rapport "IT-säkerhetsgranskning av Lupin" 2008-06-19, dnr IR 2007/13.

faktiskt har. På LU lagras omfattande informationsmängder på olika håll, bland annat inom forskningsverksamheten. Kunskapen om informationens skyddsvärde och karaktär bedöms dock vara låg. För LU bör det vara angeläget att säkerställa att all information har en ansvarig ägare och ges rätt skydd avseende sekretess, riktighet, tillgänglighet och spårbarhet.

LU saknar en formaliserad rutin för rapportering och hantering av informationssäkerhetsincidenter. Enligt uppgift ska all incidenthantering kopplad till IT-/informationssäkerhet skötas av LDC, men granskningen visar att alla incidenter inte når LDC. Därmed finns det inte någon samlad bild över inträffade informationssäkerhetsincidenter på LU, vilket försvårar analys av inträffade incidenter och preventiva åtgärder för att motverka incidenter.

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

Riksrevisionen *rekommenderar* LU att införa rutiner för informationsklassning. För att uppnå en samlad bild över inträffade informationssäkerhetsincidenter på LU bör rutiner för incidenthantering fastställas.

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. De kan vara både manuella och automatiska. Ytterst ska kontrollåtgärder bidra till att myndigheten når sina mål och att ledningens direktiv för verksamheten genomförs. Kontrollåtgärder kan ske på alla nivåer i organisationen.

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

Granskningen visar att det i flera fall saknas fastställda rutinbeskrivningar för hantering av behörigheter. Detta kan vara en följd av att det inte finns några universitetsgemensamma riktlinjer för hantering av behörigheter. Konsekvensen blir att det saknas förhindrande kontroller som säkerställer att det inte förekommer obehörig tillgång till information samt olämplig fördelning av arbetsuppgifter. Detta gäller inte minst för privilegierade användare såsom system-, databas- och operativsystemadministratörer, utvecklare samt konsulter som ofta har åtkomst till verksamhetskritiska system.

Formaliserade rutiner för kontinuitets- och avbrottsplanering finns inte på LU. Ansvaret för kontinuitetsplanering uppges ligga på systemägarna, men detta ansvar har inte tydligt kommunicerats till dessa. Granskningen visar att det inom verksamheten finns uppfattningar om att det är LDC som är ansvarig för kontinuitets- och avbrottsplanering. När ansvaret inte finns

definierat ökar risken för att arbetsuppgifter hamnar mellan stolar och att informationen inte skyddas och hålls tillgänglig på ett tillräckligt sätt.

LU har inte beslutat om policyer eller riktlinjer för användning av Internet, e-post, mobil kommunikation och distansarbete. LU saknar också rutiner som säkerställer att all elektronisk information har virusskydd och är föremål för systematisk säkerhetskopiering. I och med LU:s decentraliserade organisation delegeras ansvaret för verksamheten, inklusive IT, till områden och institutioner. Vid granskningen har det framkommit att virusskydd, säkerhetskopiering och återläsningstest inte tillämpas på ett systematiskt och fullständigt sätt på alla institutioner.

Riksrevisionen *rekommenderar* LU att med riskanalyser som grund på ett mer systematiskt sätt arbeta med dokumenterade kontrollåtgärder för att motverka identifierade risker inom informationssäkerhetsområdet.

Riksrevisionen *rekommenderar* LU att fastställa rutiner för behörighetshantering och kontinuitetsplanering samt rutiner som säkerställer säkerhetskopiering, återläsningstester och att materialet skyddas från yttre påverkan.

3.4 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. Ledningen behöver säkerställa att information når fram och inte fastnar på vägen. Behovet av tydlighet och kommunikation är stort i organisationer där verksamheten är geografiskt utspridd och samarbete sker både vertikalt och horisontellt. Ansvaret för en fungerande kommunikation ligger på ledningen.

Merparten av de intervjuade uppger att styrning och information från ledningen eller universitetsförvaltningen i informationssäkerhetsfrågor är låg. Föreskrifter för IT-säkerhet från 2003 upplevs som otydliga och har inte kompletterats med förtydliganden i anvisningar eller utbildningsinsatser i samband med att de beslutades.

Universitetsförvaltningen upplever att information om ansvar, roller och arbetsuppgifter är kommunicerad, medan verksamheten anger att den inte har fått denna information. Enligt uppgift sprids information i olika forum och grupper, men den dokumenteras inte och delges inte verksamheten på ett strukturerat sätt.

Riksrevisionen *rekommenderar* LU att införa rutiner som säkerställer att information sprids och utbildning ges till verksamheten i informationssäkerhetsfrågor på ett strukturerat sätt. När riktlinjer och anvisningar för informationssäkerhet är beslutade bör en informations- och utbildningsplan fastställas så att systemägare, prefekter och andra användare får den information och kunskap som de behöver för att kunna utföra sina arbetsuppgifter kopplade till informationssäkerhet. På motsvarande sätt behöver utbildning ges i den modell för systemförvaltning som ska införas.

3.5 Uppföljning

Uppföljning bör genomföras på alla nivåer i organisationen för att säkerställa måluppfyllelse och att risker hanterats enligt beslut. Omfattning och frekvens beror i första hand på värderingen av identifierade risker och verksamhetens komplexitet. Ledningen är ansvarig 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 kan följas upp.

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

Av Vervas föreskrifter 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. På LU finns ingen utsedd person som ansvarar för samordning av arbetet med informationssäkerhet, och därför görs inte heller någon sådan redovisning.

Riksrevisionens granskning visar att det inte förekommer några systematiska uppföljningsaktiviteter av informationssäkerheten inom LU. Precis som för styrning av informationssäkerheten uppger merparten av de intervjuade att förekomsten av uppföljning är låg. Även universitetsförvaltningen uppger att någon systematisk uppföljning av informationssäkerhetsfrågor inte görs.

Det är Riksrevisionens bedömning att det föreligger väsentliga uppföljningsbehov för att säkerställa att LU har en tillfredsställande nivå på informationssäkerheten.

Riksrevisionen har vid flera tillfällen rapporterat om brister i LU:s system för att följa upp delegerat ansvar.[6] I granskningar har Riksrevisionen konstaterat att beslutade policyer och riktlinjer inte följs av verksamheten. Detta är en generell iakttagelse som även gäller för informationssäkerheten. I LU:s decentraliserade organisation förekommer delegering av ansvar i flera led. Det är dock alltid ledningen som är ytterst ansvarig för att verksamheten bedrivs effektivt och i enlighet med gällande regelverk.

Riksrevisionen *rekommenderar* LU 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.

---

[6] Exempelvis i Revisionsrapport om uppdragsutbildning 2008-03-12, i Revisions-PM om bl.a. inköp och upphandling 2009-04-06, i Revisions-PM 2007-04-20 om bl.a. lärares bisysslor och beslut om kontroll av tidiga avbrott på kurs samt i Revisions-PM 2006-04-27 om bl.a. rutiner för hantering av externa medel och inventering av anläggningstillgångar.

Riksrevisionen *rekommenderar* LU att i beslut om riktlinjer och anvisningar för informationssäkerhet fastställa ansvar för dokumenterad och regelbunden uppföljning. Denna rekommendation gäller även andra områden än informationssäkerhet där det i dag saknas tydligt ansvar för uppföljning av att beslutade policyer och riktlinjer följs.

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

Christina Fröderberg

Ulrika Meyer

Kopia för kännedom:

Regeringen
Internrevisionen, Lunds universitet