Karolinska institutet
171 77 Stockholm

Datum 2011-02-01
Dnr 32-2010-0715

Granskning av intern styrning och kontroll av informationssäkerheten vid Karolinska institutet 2010

Riksrevisionen har som ett led i den årliga revisionen av Karolinska institutet (KI) granskat intern styrning och kontroll av informationssäkerheten.

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

Riksrevisionen önskar information senast 2011-04-15 med anledning av våra iakttagelser i denna rapport.

1. Sammanfattning

Genomförd granskning av den interna styrningen och kontrollen av informationssäkerheten vid KI visar på brister som behöver åtgärdas. Riksrevisionen har därvid följande rekommendationer:

- KI bör fastställa en policy för informationssäkerhet och komplettera med riktlinjer så att myndigheten får ett ramverk för styrning och uppföljning av informationssäkerhet som motsvarar etablerad standard inom området.
- En informationssäkerhetschef bör utses som har ansvar för samordning av arbetet med informationssäkerhet.
- Riskanalys för informationssäkerhet bör genomföras och beslut bör tas om hur identifierade risker ska prioriteras och hanteras.
- I riskanalysen bör beaktas informationens skyddsvärde med hjälp av informationsklassningar, rapporterade incidenter och uppföljningar.
- Med riskanalysen som grund bör KI på ett systematiskt sätt arbeta med dokumenterade kontrollåtgärder för att motverka identifierade risker inom informationssäkerhetsområdet.
- Rutiner bör fastställas för behörighetshantering och kontinuitetsplanering samt rutiner som säkerställer

säkerhetskopiering, återläsningstester och att materialet skyddas från yttre påverkan.
- KI bör fastställa avbrotts-/kontinuitetsplaner för de verksamheter och system som är väsentliga för lärosätets verksamhet samt fastställa rutiner för incidenthantering även på lokal nivå.
- KI bör införa rutiner för att systematiskt sprida information till olika personalkategorier inom området informationssäkerhet.
- KI bör på ett systematiskt sätt utifrån genomförda riskanalyser och kontrollåtgärder följa upp informationssäkerheten. En sammanställd redovisning av genomförda uppföljningar bör redovisas till styrelsen.
- I beslut om riktlinjer och anvisningar för informationssäkerhet bör ansvar fastställas för dokumenterad och regelbunden uppföljning av regelverket.

2. 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 är en del av den interna styrningen och kontrollen. Brister i ledningens upprättande och genomförande av generella kontroller för att uppnå en god informationssäkerhet kan medföra att myndighetens interna styrning och kontroll försvagas.

3. Normgivande regelverk

De normer som Riksrevisionen använt sig av vid bedömningen är

- Högskoleförordning 2003:100
- Förordning (2003:770) om statliga myndigheters arbete med säkert elektroniskt informationsutbyte.
- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10)
- Commitee of Sponsoring Organizations of the Treadway Commission (COSO).

Av 2 kapitlet § 2 i högskoleförordningen framgår att det är styrelsens ansvar att säkerställa att det vid högskolan finns en intern styrning och kontroll som fungerar på ett betryggande sätt.

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). Denna ersattes 2010-02-01 av MSB föreskrift MSBFS 2009:10.

För att beskriva intern styrning och kontroll har den så kallade COSO-modellen blivit ett vedertaget begrepp. COSO beskriver intern styrning och kontroll i olika komponenter och deras inbördes samband. Komponenterna i COSO är kontrollmiljö, riskanalys, kontrollåtgärder, information/kommunikation och uppföljning.

4. Iakttagelser och rekommendationer

4.1 Kontrollmiljö

Kontrollmiljön är grundförutsättningen för intern styrning och kontroll i en organisation och de andra COSO-komponenterna. Med kontrollmiljö avses bl.a. ledningens filosofi, attityder/inställning och ledarstil, hur ledningen delegerar ansvar och befogenheter, organiserar och utvecklar medarbetare samt följer upp fattade beslut. En viktig komponent i kontrollmiljön är organisationskulturen. Med organisationskultur menas vilken kultur som finns i organisationen, där öppenhet och intresse från ledningen för kontrollfrågor är mycket viktiga, då den påverkar medarbetares engagemang och medvetenhet.

Av MSB:s föreskrift (4 §) framgår att en myndighet ska i sitt arbete med att upprätthålla säkerhet i sin informationshantering tillämpa ett ledningssystem för informationssäkerhet. Det innebär bland annat att myndigheten ska upprätta en informationssäkerhetspolicy 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. Informationssäkerhet vid KI ska inbegripa all säkerhet kring lärosätets informationsbehandling, såväl organisatoriska åtgärder som fysiska och logiska skyddsåtgärder. Exempel på säkerhetsrelaterade åtgärder är en fastställd informationssäkerhetspolicy, ansvarsfördelning, utbildning, riskanalys, katastrofplan, behörighetsregler, informationsklassning, säkrad driftmiljö, behörighetsadministration, säkerhetskopiering etc. Informationssäkerheten ska motverka risker för såväl obehörig läsning och

förändring av data som förlust av data. Informationssäkerheten syftar även på informationens kvalitet, riktighet och tillgänglighet.

Riksrevisionens granskning har visat att det vid KI finns ett ramverk i form av regler och riktlinjer för IT-säkerhet och anvisningar för datoranvändning vid KI. Dessa dokument reglerar IT-säkerheten snarare än informationssäkerheten. Väsentliga riktlinjer som bör finnas i ett LIS saknas, t.ex. informationssäkerhetspolicy, riktlinjer för riskanalys, informationsklassning, incidenthantering, hantering av behörigheter, metod för utveckling och ändring av system, hantering av drift- och e-kommunikation, kontinuitetsplanering samt avbrottsplaner för system och nätverk.

Lärosätet ska även enligt MSB:s föreskrift (4 §) utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet. I KI:s regler och riktlinjer för IT-säkerhet vid lärosätet anges att universitetsdirektören har det yttersta ansvaret för IT-säkerheten vid universitetet i enlighet med rektors delegation. Prefekt/motsvarande ansvarar för IT-säkerheten vid institutionen/motsvarande. Om särskild systemägare är utsedd, ansvarar denne för IT-säkerheten i respektive IT-system. Riksrevisionens granskning har dock visat att det inte finns någon utsedd informationssäkerhetschef som ansvarar för säkerhetsarbetet. Ansvaret är istället delegerat till prefekt/motsvarande på institutionerna. Någon specifik befattning för informationssäkerhet var inte utsedd på institutionerna. Vid en institution fanns 13 stycken sektioner under institutionen. Den största sektionen hade en IT-samordnare medan de mindre sektionerna vände sig till IT-konsulter vid problem. Det saknades arbetsbeskrivningar för rollen som IT-samordnare. Det fanns även oklarheter i ansvar och roller mellan den centrala och lokala nivån vad avser informationssäkerheten. Några exempel är att IT centralt förutsätter att det vid den lokala nivån finns framtagna regler för incidenthantering, säker hantering av drift- och e-kommunikation, kontinuitetsplanering samt avbrottsplaner för system och nätverk. Vid de granskade institutionerna har man ansett att det åligger den centrala nivån att ta fram sådana riktlinjer. Konsekvensen har blivit att sådana riktlinjer därmed har saknats.

Riksrevisionen *rekommenderar* KI att fastställa en policy för informationssäkerhet och att komplettera med riktlinjer så att myndigheten får ett ramverk för styrning och uppföljning av informationssäkerhet som motsvarar etablerad standard inom området.

Riksrevisionen *rekommenderar* KI att utse en informationssäkerhetschef som har ansvar för samordning av arbetet med informationssäkerhet.

4.2 Riskanalys

I riskanalysarbetet är organisationens mål och uppdrag den primära utgångspunkten. Av MSB:s föreskrifter framgår att myndigheten utifrån risk- och sårbarhetsanalyser och inträffade incidenter ska avgöra hur risker ska hanteras samt besluta om åtgärder för myndighetens informationssäkerhet. Riskanalysen ligger till grund för utformning av en lämplig handlingsplan och kontrollåtgärder i syfte att minska riskerna till en godtagbar nivå. Riskanalys bör genomföras på samtliga organisatoriska nivåer.

Riksrevisionens granskning har visat att det inte har genomförts någon riskanalys specifikt för informationssäkerhet. Området har dock ingått som en del i den generella riskanalysen enligt förordning (2007:603) om intern styrning och kontroll. Det har även framkommit att det inte har genomförts någon informationsklassning. Klassning av information är nödvändig för att bedöma vilket skyddsbehov som föreligger i samband med riskanalys och utformning av kontrollåtgärder. Utgångspunkt vid riskanalys och informationsklassning bör vara informationens skyddsbehov utifrån sekretess, riktighet, tillgänglighet och spårbarhet.

En väl genomförd riskanalys som beaktar informationssäkerhet är nödvändig för att relevanta kontrollåtgärder och uppföljningsaktiviteter ska kunna utformas.

Riksrevisionen *rekommenderar* KI att genomföra en riskanalys för informationssäkerhet samt besluta hur identifierade risker ska prioriteras och hanteras.

Riksrevisionen *rekommenderar* KI att i riskanalysen beakta informationens skyddsvärde med hjälp av informationsklassningar, rapporterade incidenter och uppföljningar.

4.3 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 myndigheten når sitt mål och att styrelsens/ledningens direktiv för verksamheten genomförs. Kontrollåtgärder kan ske på alla nivåer i organisationen. Dokumenterade rutinbeskrivningar är exempel på hjälpmedel i genomförandet av kontrollåtgärder.

Riksrevisionens granskning visar på brister i kontrollåtgärder som bör finnas för att lärosätet i större utsträckning ska leva upp mot ett LIS utifrån etablerad standard i området. Rutinen för ändring och uppföljning av behörigheter var bristfällig. Rutiner för hantering av behörigheter är nödvändig för att kontinuerligt försäkra sig om att ingen har högre behörighet än vad som krävs utifrån arbetsuppgiften och för att säkerställa informationens integritet. Under granskningen framkom att det inte fanns någon ensad avbrotts- och kontinuitetsplan vid lärosätet och att det saknades rutiner för incidenthantering på lokal nivå. Vidare fanns inga centrala riktlinjer eller rutiner för säkerhetskopiering. Rutinerna för säkerhetskopiering är delegerat till institutionerna. Säkerhetsrutinerna varierade mellan institutionerna. Vissa grupper hade en gemensam back-up server medan andra hade individuell backup på extern disk.

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

Riksrevisionen *rekommenderar* KI att fastställa avbrotts-/kontinuitetsplaner för de verksamheter och system som är väsentliga för lärosätets verksamhet samt fastställa rutiner för incidenthantering även på lokal nivå.

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 behöver förstå sin egen roll avseende informationssäkerhet och hur enskilda aktiviteter påverkar andra aktiviteter.

Riksrevisionens granskning har visat att det saknas regelbunden information och utbildning kring informationssäkerhet till exempelvis för IT-administratörer eller vanliga användare inom området informationssäkerhet. Det är upp till institutionsledningen att låta sin personal gå utbildning. Utbildningsinsatserna varierar därmed mellan institutionerna.

Riksrevisionen bedömer att det finns ett behov av riktad/anpassad och kontinuerlig informationsspridning för att underlätta efterlevnad av regelverk.

Riksrevisionen *rekommenderar* KI att införa rutiner för att systematiskt sprida information till olika personalkategorier inom området informationssäkerhet.

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. Styrelse/ledning är ansvariga för uppföljning och utvärdering av verksamhetens interna styr- och kontrollsystem. För informationssäkerhet är policy, riktlinjer och rutiner ledningens fastställda kriterier mot vilka intern styrning och kontroll följs upp.

Av MSB:s föreskrift (4 §) framgår att det ska utses en eller flera personer som leder och samordnar arbetet med informationssäkerhet. Vidare framgår av föreskriften (5 §) att myndighetens ledning löpande ska informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet på myndigheten. På KI finns ingen utsedd informationssäkerhetschef som ansvarar för samordning av arbetet med informationssäkerhet och därför görs inte heller någon sådan dokumenterad utvärdering.

Granskningen har visat att det inte förekommer några systematiska uppföljningsaktiviteter från ledningsnivån. Det saknas således en central styrning av lärosätets informationssäkerhet. Uppföljning centralt sker endast vid incidenter.

Riksrevisionen *rekommenderar* KI att på ett systematiskt sätt utifrån genomförda riskanalyser och kontrollåtgärder följa upp informations-

säkerheten. En sammanställd redovisning av genomförda uppföljningar bör redovisas till styrelsen.

Riksrevisionen *rekommenderar* KI att i beslut om riktlinjer och anvisningar för informationssäkerheten fastställa ansvar för dokumenterad och regelbunden uppföljning av regelverket.

Ansvarig revisor Per Flodman har beslutat i detta ärende. Uppdragsledare Iréne Lindström har varit föredragande.

Per Flodman Iréne Lindström

Kopia för kännedom:
Regeringen