Revisionsrapport

RIKSREVISIONEN

Högskolan Kristianstad
291 88 Kristianstad

Datum 2010-03-18
Dnr 32-2009-0642

Granskning av intern styrning och kontroll av informationssäkerheten vid Högskolan Kristianstad 2009

Riksrevisionen har som ett led i den årliga revisionen granskat Högskolan Kristianstads (Hkr) interna styrning och kontroll av informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa Hkr:s uppmärksamhet på i denna rapport.

Riksrevisionen önskar information senast 2010-05-03 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 revisionsår 2009 som ett led i den årliga revisionen granskat hur Hkr arbetar med intern styrning och kontroll av informationssäkerhet.

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 en säker hantering av informationstillgångarna kan visas.

Riksrevisionens granskning visar att Hkr saknar ett ramverk för styrning av informationssäkerheten vid högskolan. Det finns inte någon utsedd person som ansvarar för arbetet med informationssäkerhet. Riskanalyser och

informationsklassningar har inte genomförts. Dokumenterade kontrollåtgärder och rutiner för uppföljning av informationssäkerheten saknas i stor 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

- 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) [1],
- Vervas allmänna råd till föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2) [2] ,
- Commitee of Sponsoring Organizations of the Treadway Commission (COSO).

Av § 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.

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.

[1] Från och med första februari 2010 träder Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet ikraft, MSBFS 2009:10. Dessa ersätter Vervas föreskrifter.
[2] Från och med första februari 2010 träder Myndigheten för samhällsskydd och beredskaps allmänna råd om statliga myndigheters informationssäkerhet ikraft, MSBFS 2009:10. Dessa ersätter Vervas allmänna råd.

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.

3. Informationssäkerhet

3.1. Kontrollmiljö

Kontrollmiljön är grundförutsättningen för intern styrning och kontroll i organisationen 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.

Av Vervas föreskrift framgår att en myndighet i sitt arbete för ett säkert elektroniskt informationsutbyte ska tillämpa ett LIS. 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. Informationssäkerhet uppnås genom att lämpliga styrmedel införs. Dessa kan vara t.ex. policy, riktlinjer, rutiner, organisation och programfunktioner.

Riksrevisionens granskning visar att det vid Hkr saknas en policy för styrning och uppföljning av informationssäkerheten. Väsentliga riktlinjer som bör finnas i ett LIS saknas, t.ex. riktlinjer för riskanalys, informationsklassning, incidenthantering, hantering av behörigheter, metod för utveckling och ändring av system, fysisk säkerhet (skalskydd).

Ledningen har inte i tillräcklig utsträckning kunskap om vilka informationstillgångar som finns i verksamheten och vilket skyddsvärde den har. Det saknas riktlinjer för informationsklassning och det finns inte någon tradition av att genomföra klassningar. Utan klassning går det inte att med rimlig säkerhet bedöma informationens skyddsvärde och vilka åtgärder som behöver vidtas för att undvika negativa konsekvenser för högskolan. Vid granskningstillfället har inte Hkr kunnat visa någon aktuell dokumentation över informationssystem vid högskolan och dokumentation som visar vilka som är systemägare och förvaltare för dessa.

Myndigheten ska enligt Vervas föreskrift utse en eller flera personer som ansvarar för säkerhetsarbetet och som minst en gång per år för myndighetsledningen redovisar och dokumenterar vilka granskningar och skyddsåtgärder av större betydelse som har vidtagits enligt myndighetens policy och styrdokument. Någon utsedd person som ansvarar för arbetet med informationssäkerhet finns inte vid Hkr. Enligt uppgift har en IT-

säkerhetssamordnare utsetts. Hkr har inte kunnat visa beslut om befattning eller det ansvar och befogenhet som personen i fråga kommer att ha.

Riksrevisionen *rekommenderar* Hkr att 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.

Riksrevisionen *rekommenderar* Hkr att utse en person som ansvarar för arbetet med informationssäkerhet på myndighetsövergripande nivå.

3.2. Riskanalys

I riskanalysarbetet är organisationens mål och uppdrag den primära utgångspunkten. 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.

Utgångspunkten för informationssäkerhetsarbetet är att riskanalyser genomförs för att kartlägga den säkerhetsnivå som ska gälla för skydd av informationen. Informationsklassningar, rapporterade incidenter och uppföljningar är viktiga informationskällor för att upprätta en bra riskanalys. Ett effektivt riskanalysarbete förutsätter kunskaper från både kärnverksamhet och IT-, informationssäkerhetsområdet.

Av Vervas föreskrift framgår att myndigheten ska, utifrån risk- och sårbarhetsanalyser och dokumenterade incidenter, avgöra vilka risker som ska elimineras, reduceras eller accepteras, samt besluta om åtgärder för myndighetens informationssäkerhet.

Riksrevisionens granskning har visat att Hkr inte har genomfört någon riskanalys för informationssäkerhet. Det har även framkommit att det inte 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 är nödvändig för att relevanta kontrollåtgärder och uppföljningsaktiviteter ska kunna utformas.

Riksrevisionen *rekommenderar* Hkr att genomföra en riskanalys för informationssäkerhet samt besluta om hur identifierade risker ska hanteras.

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

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. Ytterst ska kontrollåtgärder bidra till att myndigheten når sina mål och att styrelsens/ledningens direktiv för verksamheten genomförs. Kontrollåtgärder kan ske på alla nivåer i organisationen.

Riksrevisionens granskning visar på avsaknad av kontrollåtgärder som bör finnas för att högskolan ska leva upp mot ett LIS utifrån etablerad standard i området.

Dokumenterade rutiner för hantering (tilldelning, ändring, borttag och uppföljning) av behörigheter saknas. Rutiner för hantering av behörigheter är nödvändiga för att kontinuerligt försäkra sig om att ingen har högre behörighet än vad som krävs utifrån arbetsuppgiften och för att säkerställa informationens integritet.

Riksrevisionens granskning visar att det saknas en dokumenterad kontinuitets-, avbrottsplan för IT-verksamheten. En plan är viktig då risk finns för driftstörningar och verksamheten är beroende av en fungerande datordrift. Det saknas fastställda rutiner för säkerhetskopiering som säkerställer att säkerhetskopior har en skyddad förvaring och att de testas regelbundet för återläsning.

Granskningen visar också att det saknas en fastställd förvaltningsmodell. En fastställd modell för förvaltning av system har en normerande verkan och sätter en lägsta nivå för vad som och hur system ska förvaltas. Ansvaret för systemägare och förvaltare har inte definierats. Riksrevisionen har begärt att få ta del av förvaltningsplaner för två system men inte erhållit några.
Det saknas vidare en fastställd metod för systemutveckling som säkerställer test och godkännande av ändringar innan driftsättning.

Riksrevisionen *rekommenderar* Hkr att, med riskanalyser som grund, på ett systematiskt sätt arbeta med dokumenterade kontrollåtgärder för att motverka identifierade risker inom informationssäkerhetsområdet. Riksrevisionen rekommenderar Hkr att fastställa rutiner för hantering av behörigheter, modell för förvaltning av system, avbrotts-/kontinuitetsplaner för IT-avdelningen och för de verksamheter och system som är väsentliga för högskolans verksamhet.

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. Någon riktad, anpassad informationsspridning till systemägare, administratörer eller användare förekommer inte.

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

3.5. Uppföljning

Uppföljning bör 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 och riktlinjer ledningens fastställda kriterier mot vilka intern styrning och kontroll följs upp.

Av Vervas föreskrift framgår att det ska finnas en utsedd person som ansvarar för arbetet med informationssäkerhet och som minst en gång per år för styrelsen/ledningen redovisar och dokumenterar vilka granskningar och åtgärder av större betydelse som har vidtagits enligt myndighetens policy och styrdokument. Vid Hkr finns, som tidigare nämnts, ingen utsedd person som ansvarar för samordning av arbetet med informationssäkerhet och därför görs inte heller någon sådan redovisning.

Riksrevisionens granskning har även visat att det inte förekommer några systematiska uppföljningsaktiviteter från ledningsnivå.

Riksrevisionen *rekommenderar* Hkr att på ett systematiskt sätt, utifrån genomförda riskanalyser och kontrollåtgärder, följa upp informationssäkerheten. En sammanställd redovisning av genomförda uppföljningar bör redovisas till styrelsen som är ansvarig för en betryggande intern styrning och kontroll.

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

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