Revisionsrapport

RIKSREVISIONEN

Högskolan i Skövde
Box 408
541 28 SKÖVDE

Datum 2010-02-03
Dnr 32-2009-0641

Granskning av intern styrning och kontroll av informationssäkerheten vid Högskolan i Skövde 2009

Riksrevisionen har som ett led i den årliga revisionen granskat Högskolans i Skövde (HS) interna styrning och kontroll av informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill uppmärksamma HS på i denna rapportering.

Riksrevisionen önskar information senast 2010-03-15 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 som ett led i den årliga revisionen granskat hur HS arbetar med intern styrning och kontroll av informationssäkerhet.

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 HS. Av policyn framgår att det kommer att finnas komplement i form av anvisningar

och instruktioner. Dessa har dock ännu inte tagits fram. HS bör ta fram riktlinjer för att ramverket i större utsträckning ska motsvara etablerad standard.

HS har inte genomfört någon dokumenterad riskanalys eller informationsklassning för informationssäkerhet. Granskningen visar också att det i stor utsträckning saknas dokumenterade kontrollåtgärder och att uppföljning av informationssäkerheten inte genomförts.

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

- 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) [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.

[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.

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.

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 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.

Av Vervas tillämpningsföreskrift 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 till exempel policy, riktlinjer, rutiner, organisation och programfunktioner.

Riksrevisionens granskning visar att HS har ett ramverk i form av beslutad policy för informationssäkerhet men att denna inte har kompletterats med riktlinjer. Väsentliga riktlinjer som bör finnas i ett LIS saknas, t.ex. riktlinjer för hantering av behörigheter, informationsklassning, incidenthantering, skalskydd för datahallar och loggning (spårbarhet).

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

3.2. Riskanalys

I riskanalysarbetet är organisationens mål och uppdrag den primära utgångspunkten. I analysen ingår att identifiera, värdera och att aktivt ta ställning till hur riskerna ska hanteras, dvs. eliminera, reducera eller acceptera. 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. Informationsklassning, 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 tillämpningsföreskrift 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 visar att det inte har genomförts någon riskanalys för informationssäkerhet. Enligt uppgift från HS genomfördes en riskanalys 2006 men att denna inte dokumenterades. Det har även framkommit att det inte genomförts någon informationsklassning. Klassning av information är nödvändig för att bedöma vilket skyddsvärde som föreligger i samband med riskanalys och utformning av kontrollåtgärder. Utgångspunkt för informationsklassning bör vara informationens skyddsbehov utifrån sekretess, riktighet, tillgänglighet och spårbarhet.

Vissa institutioner på HS har egna serverar, databaser som är placerade på fysiskt och virtuellt på institutionerna. Från ledningens sida saknas kunskap om hur denna information skyddas och om riskanalyser genomförs för dessa informationssystem.

Riksrevisionen *rekommenderar* HS 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 HS samt riskanalyser för specifika system.

Riksrevisionen *rekommenderar* HS 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 universitetet når sina mål och att styrelsens/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.

Dokumenterade rutiner för behörigheter är en förutsättning för ett systematiskt arbete med att tilldela, ändra, ta bort och följa upp behörigheter. Granskningen visar att dokumenterade rutiner för hantering av behörigheter saknas på central nivå och att det inte görs någon regelbunden eller dokumenterad uppföljning av behörigheter, vilket är förenat med risker för hela myndigheten.

Granskningen visar att HS saknar dokumenterade och fastställda kontinuitets-/avbrottsplaner för sina informationssystem.

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

Riksrevisionen *rekommenderar* HS att fastställa rutiner för hantering av behörigheter, kontinuitets-/avbrottsplaner 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 om mål, risker, ansvar, befogenheter och rutiner.

Ledningen uppfattar att information om ansvar, roller och arbetsuppgifter är kommunicerade i verksamheten genom att informationssäkerhetspolicyn finns tillgänglig på högskolans hemsida. Dessutom har IT-chefen fortlöpande informationsmöten med prefekter och enhetschefer om IT-området och därmed även informationssäkerhet.

Av informationssäkerhetspolicyn framgår att information och utbildning inom säkerhetsområdet ska ske fortlöpande och vid all nyanställning. Den fortlöpande informationen och utbildningen sker dock endast till ny personal och nya studenter. Dessa får då även skriva på ett användaravtal.

Riksrevisionen *rekommenderar* HS att införa rutiner för att systematiskt utbilda personal och studenter om informationssäkerhet.

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.

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 HS 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. Det fanns inte vid granskningstillfället någon utsedd person med ansvar för uppföljningen av informationssäkerheten.

Riksrevisionens granskning visar att det inte förekommer några systematiska uppföljningar av informationssäkerheten från ledningsnivå.

Riksrevisionen *rekommenderar* HS 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* HS 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 Nenus Jidah har varit föredragande.

Christina Fröderberg Nenus Jidah

Kopia för kännedom:

Regeringen