Malmö Högskola
205 06 Malmö

Datum 2012-05-22
Dnr 32-2011-0688

Granskning av intern styrning och kontroll av informationssäkerheten vid Malmö Högskola 2011

Riksrevisionen har som ett led i den årliga revisionen av Malmö Högskola (MaH) granskat den interna styrningen och kontrollen av informationssäkerheten för 2011.

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

Riksrevisionen önskar information senast 2012-06-30 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 2011 som ett led i den årliga revisionen granskat hur MaH arbetar med intern styrning och kontroll av informationssäkerhet.

Riksrevisionen bedömer att vissa åtgärder vidtagits på ledningsnivå för att åstadkomma ett LIS, men att åtgärderna inte är tillräckliga och att de inte kommunicerats och implementerats i verksamheten fullt ut. 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. Intern styrning och kontroll förutsätter en god informationssäkerhet och säker hantering av information. 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.

MaH bör införa åtgärder för att ramverket av styrande dokument och kontroller i större utsträckning ska motsvara etablerad standard. Informationssäkerhetspolicy saknas och det finns inte någon utsedd person som ansvarar för arbetet med informationssäkerhet.

MaH 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. Informationssäkerhet

1.1 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 i övrigt försvagas. För att påvisa en god intern styrning och kontroll förutsätts också en säker hantering av informationstillgångarna.

1.2 Normgivande regelverk

De normer som Riksrevisionen har använt sig av vid sin bedömning är

- Förordningen (2007:603) om intern styrning och kontroll (FISK)
- Myndighetsförordningen (2007:515)
- Högskoleförordning (2003:100)
- Förordning (2003:770) om statliga myndigheters arbete med säkert elektroniskt informationsutbyte,
- Myndigheten för samhällsskydd och beredskaps föreskrifter (2009:10) om statliga myndigheters informationssäkerhet.
- Ramverk från Committee 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 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.

Mot bakgrund av det ökade elektroniska informationsutbytet i samhället gav den dåvarande myndigheten 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. Myndigheten för samhällsskydd och beredskap (MSB) utgav 2009 en uppdaterad föreskrift.

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

1.3 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 MSB:s 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. Informationssäkerhet uppnås genom att lämpliga styrmedel införs. Dessa kan vara till exempel policy, riktlinjer, rutiner, organisation och programfunktioner.

Riksrevisionens granskning visar att MaH inte har någon beslutad informationssäkerhetspolicy eller underliggande rutiner. Det finns inte heller någon utsedd ansvarig för informationssäkerhet på högskolan. Ansvaret är i dagsläget i praktiken delat mellan avdelningarna Bibliotek & IT (BIT) samt kommunikationsavdelningen.

Väsentliga riktlinjer som bör finnas i ett LIS saknas, t.ex. riktlinjer för hantering av behörigheter, informationsklassning och incidenthantering.

Ledningen har inte i tillräcklig utsträckning kunskap om vilka informationstillgångar som finns ute på centrum, fakultets- och områdesnivå, var informationen finns och vilket skyddsvärde den har. Riktlinjer för informationsklassning saknas och 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.

Rekommendation

Riksrevisionen rekommenderar MaH att fastställa en informationssäkerhetspolicy och att kompletterande riktlinjer tas fram för att få ett komplett ramverk för informationssäkerhet som motsvarar etablerad standard inom området.

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

Av MSB:s 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.

Vissa områden på MaH har egna servrar och databaser. Det fanns ingen kunskap på ledningsnivå om säkerhetsbehovet för dessa informationssystem.

Riksrevisionens granskning har visat att det inte genomförts några riskanalyser för informationssäkerhet och det har inte heller genomförts informationsklassning av informationen.

Rekommendation

Riksrevisionen rekommenderar MaH 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 MaH samt riskanalyser för specifika system.

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

1.5 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 MaH når sina mål och att ledningens direktiv för verksamheten genomförs. Kontrollåtgärder ska ske på alla nivåer i organisationen.

Riksrevisionens granskning visar att förekomsten av dokumenterade kontrollåtgärder är låg. Säkerhetskopiering sker av centrala system på MaH, det finns dock även system som hanteras lokalt på områden. BIT erbjuder backup av dessa men MaH har ingen kunskap om dessa system säkerhetskopieras på ett tillfredsställande sätt.

MaH har ingen formaliserad process för behörighetshantering. Behörigheter bör hanteras enligt en centralt beslutad process för högskolans samtliga system.

MaH utvecklar inte några egna IT-system enligt en policy beslutad av ledningen. Det finns ingen beslutad process för systemutveckling och ändringshantering på högskolan. Det är ändå väsentligt att en central styrning finns av systemutveckling och ändringshantering för att säkerställa en säkerhet i högskolans IT-miljö. Detta eftersom stora delar av anpassning av inköpta system sker på områdesnivå.

Det finns inte heller kontinuitetsplaner och avbrottsplaner för högskolans samtliga system. Högskolan har påbörjat ett arbete med att kartlägga och klassificera sina system och har uppgett att kontinuitetsplaner och avbrottsplaner ska tas fram i samband med detta.

Rekommendation

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

Riksrevisionen rekommenderar MaH att fastställa rutiner för hantering av behörigheter, systemutveckling och ändringshantering, kontinuitets-/avbrottsplaner samt rutiner som säkerställer säkerhetskopiering.

1.6 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 befintligt regelverk kring informationssäkerhet finns på intranätet.

MaH genomför inte några strukturerade utbildningar till ledning, övrig personal eller studenter avseende informationssäkerhet. MaH har angett att en IT-strateg ska anställas på rektorns stab och att detta ska ligga inom dennes ansvarsområde.

Rekommendation

Riksrevisionen rekommenderar MaH att införa rutiner för att systematiskt utbilda personal och studenter inom området informationssäkerhet.

1.7 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 MSB:s föreskrift 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 MaH finns ej någon utsedd person som ansvarar för samordning av arbetet med informationssäkerhet.

Riksrevisionens granskning visar att det inte förekommer några systematiska uppföljningar av informationssäkerheten från centralt håll eller på områdena.

Rekommendation

Riksrevisionen rekommenderar MaH 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 MaH 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

Utbildningsdepartementet

Finansdepartementet (budgetavdelningen)