Blekinge Tekniska Högskola
371 79 KARLSKRONA

Datum 2010-01-26
Dnr 32-2009-0637

Granskning av intern styrning och kontroll av informationssäkerheten vid Blekinge Tekniska Högskola 2009

Riksrevisionen har som ett led i den årliga revisionen granskat Blekinge Tekniska Högskolas (BTH) interna styrning och kontroll av informationssäkerhet.

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

Riksrevisionen önskar information senast 2010-03-08 med anledning av våra iakttagelser i denna rapportering.

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 BTH 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 har 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 högskolan har en policy för IT-säkerhet som tydligt beskriver ansvar och roller. Policyn behöver kompletteras med fler riktlinjer för att i större utsträckning motsvara etablerad standard. Det finns inte heller någon utsedd person som ansvarar för arbetet med

informationssäkerhet vid BTH. Riskanalys och informationsklassning har inte genomförts vid BTH. Granskningen visar också att det i stor utsträckning saknas dokumenterade kontrollåtgärder och att uppföljning av informationssäkerheten inte genomförs.

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),
- Vervas allmänna råd till föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2),
- 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.

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 tillämpningsföreskrift framgår det 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 BTH har en IT-säkerhetspolicy för användning av datorer och kommunikationsteknik. Policyn beskriver i viss utsträckning hur information ska skyddas. Granskningen visar dock att 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, skalskydd för datahallar. Nuvarande policy och riktlinjer behöver kompletteras för att i större utsträckning återspegla ett LIS enligt etablerad standard inom området informationssäkerhet.

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. Högskolans IT-säkerhetspolicy beskriver tydligt ansvar och roller för informationssäkerhet. Befattningen IT-säkerhetshandläggare har en mycket viktig roll i policyns beskrivning av viktiga säkerhetsmoment. Riksrevisionens granskning visar dock att det inte finns någon person vid BTH som har denna befattning. Enligt uppgift kommer en person att tilldelas ansvaret för arbetet med informationssäkerhet.

Riksrevisionen *rekommenderar* BTH att utveckla nuvarande policy och komplettera med riktlinjer för att få ett ramverk för styrning och uppföljning av informationssäkerhet som i högre utsträckning motsvarar etablerad standard inom området.

Riksrevisionen *rekommenderar* BTH 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. I analysen ingår att identifiera, värdera och att aktivt ta ställning till hur risker ska hanteras, d v s 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. Informationsklassningar, rapporterade incidenter och uppföljningar är viktiga informationskällor för att upprätta en bra riskanalys. Ett effektivt riskanalysarbete med avseende på informationssäkerhet 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 har visat att det inte genomförts 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 som beaktar informationssäkerhet är nödvändig för att relevanta kontrollåtgärder och uppföljningsaktiviteter ska kunna utformas.

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

Riksrevisionen *rekommenderar* BTH 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. Dokumenterade rutinbeskrivningar är exempel på hjälpmedel i genomförandet av kontrollåtgärder.

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

Dokumenterade rutiner för hantering (tilldelning, ändring, borttag och uppföljning) av behörigheter saknas. BTH saknar också fastställda rutiner för hantering av privilegierade behörigheter för databaser, operativsystem mm. 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.

Högskolans IT-säkerhetspolicy reglerar att det ska finnas avbrottsplanering för system av stor betydelse för säkerhet, ekonomi, utbildning eller forskning samt för centrala eller gemensamma system. Det framgår också av policyn att systemägarna ska genomföra planeringen. Under granskningen framkom att det inte finns några fastställda planer för viktiga system för att hantera avbrott eller för att säkra verksamhetens kontinuitet.

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

Riksrevisionen *rekommenderar* BTH att fastställa rutiner för hantering av behörigheter, avbrotts-/kontinuitetsplaner samt rutiner som säkerställer säkerhetskopiering, återläsningstester och att materialet skyddas från yttre påverkan bör fastställas.

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. Någon riktad, anpassad informationsspridning till systemägare, administratörer eller användare för att säkerställa efterlevnad av regelverk förekommer inte.

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

3.5. 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 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. På BTH finns som nämnts tidigare ingen utsedd person som ansvarar för samordning av arbetet med informationssäkerhet och därför görs inte heller någon sådan redovisning.

Granskningen har även visat att det inte förekommer några systematiska uppföljningsaktiviteter från ledningsnivå samt att det inte heller genomförs några systematiska uppföljningsaktiviteter på IT-avdelningen.

Riksrevisionen *rekommenderar* BTH 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* BTH 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 Mikael Pettersson har varit föredragande.

Christina Fröderberg

Mikael Pettersson

Kopia för kännedom:

Regeringen