Revisionsrapport

RIKSREVISIONEN

Växjö universitet
Box 451
351 06 VÄXJÖ

Datum 2010-02-25
Dnr 32-2009-0646

Granskning av intern styrning och kontroll av informationssäkerheten vid Växjö universitet 2009

Riksrevisionen har som ett led i den årliga revisionen 2009 granskat Växjö Universitets (VXU) interna styrning och kontroll av informationssäkerhet.

Den 1 januari 2010 bildade VXU tillsammans med Högskolan i Kalmar Linnéuniversitetet. De iakttagelser som granskningen har resulterat i och som redovisas i denna revisionsrapport bör tas till vara vid utformningen av informationssäkerheten vid Linnéuniversitetet.

Riksrevisionen önskar information senast 2010-03-25 med anledning av våra iakttagelser i denna rapport.

1. 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 granskat hur VXU arbetar med ett LIS och i vilken utsträckning detta arbete är integrerat med myndighetens interna styrning och kontroll.

Riksrevisionen bedömer att vissa åtgärder vidtagits på ledningsnivå men att åtgärderna inte är tillräckliga. 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 vid VXU saknas ett ramverk för styrning och uppföljning av informationssäkerhet och att policys och riktlinjer behöver tas fram för att få ett LIS som motsvarar etablerad standard. Vissa av universitetets institutioner har tagit fram IT-policys, dock inte alla.

VXU har inte genomfört riskanalyser för informationssäkerhet på universitetsövergripande nivå. Därför saknas en sammanställd bild över vilka risker som bör prioriteras vid VXU. Det var vid granskningstillfället inte tydligt hur informationssäkerhetsrisker tas om hand i de riskanalyser som genomförs inom ramen för förordning om intern styrning och kontroll (FISK).

Det saknades i stor utsträckning dokumenterade kontrollåtgärder för informationssäkerheten.

Granskningen visar också att rutiner saknas för uppföljning inom området och att uppföljning ej genomförts av universitetets styrelse/ledning. Det fanns inte heller någon av styrelsen/ledningen utsedd som ansvarig för universitetets uppföljning av informationssäkerhet.

För att universitetets styrelse/ledning ska ha ett relevant och tillförlitligt underlag vid bedömning av den interna styrningen och kontrollen behöver arbetet med LIS integreras i arbetet enligt förordningen om intern styrning och kontroll (FISK) i en högre utsträckning.

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 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.

3. Normgivande regelverk

De normer som Riksrevisionen använt sig av vid bedömningen är

- Förordning (2007:603) om intern styrning och kontroll (FISK),
- 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).

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 universitetet 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. FISK bygger sin struktur på COSO som 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. 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.

4. Informationssäkerhet

4.1. 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

[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.

organisationskulturen då den påverkar medarbetares engagemang och medvetenhet.

Riksrevisionens granskning visar att det vid VXU inte finns någon universitetsövergripande beslutad informationssäkerhetspolicy eller IT-policy. Ett par av universitetets institutioner har skapat policydokument avseende IT-säkerhet, dock inte alla.

Riktlinjer för användning av internet och e-post fanns på universitetet, men avsåg endast studenter. Det bör från ledningsnivå tydligt visas vad som förväntas av anställda när det gäller internetanvändning, etik, etc.

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

Ledningen har inte i tillräcklig utsträckning kunskap om vilka informationstillgångar som finns ute på institutions-, avdelningsnivå, 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 universitetet.

Riksrevisionen *rekommenderar* att informationssäkerhetspolicy ska fastställas och att kompletterande riktlinjer tas fram för att få ett komplett ramverk för informationssäkerhet som motsvarar etablerad standard inom området.

4.2. Riskanalys

I riskanalysarbetet är organisationens mål och uppdrag den primära utgångspunkten. Riskanalysen är grunden för att utforma en lämplig åtgärdsplan 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. 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 full ut beaktas i arbetet med FISK finns risk för att styrelsens/ledningens underlag för bedömning av den interna styrningen och kontrollen inte är tillförlitligt.

VXU har inte genomfört någon riskanalys för informationssäkerhet på universitetsövergripande nivå. Vervas tillämpningsföreskrift föreskriver att en myndighet utifrån risk- och sårbarhetsanalyser och dokumenterade incidenter ska avgöra vilka risker som ska elimineras, reduceras eller accepteras, samt besluta om åtgärder för myndighetens informationssäkerhet. Informationssäkerhet har ej beaktats i samband med riskanalysen i FISK-

arbetet. Detta innebär att personer med ansvar för och kunskap om informationssäkerhet inte varit involverade i den genomförda riskanalysen (FISK).

Ett flertal institutioner på VXU har egna servrar, databaser som är placerade både fysiskt och virtuellt på institutionerna. Det fanns ingen kunskap på ledningsnivå om säkerhetsbehovet för dessa informationssystem. Vid granskningstillfället uppgav ansvariga för informationssäkerheten att det inte genomförts några dokumenterade riskanalyser eller informationsklassningar för informationssystemen.

Riksrevisionen *rekommenderar* att riskanalyser för informationssäkerhet genomförs och att beslut fattas om hur identifierade risker ska hanteras. Riskanalysen bör ha sin grund i riskanalyser genomförda på lägre nivåer samt riskanalyser för specifika system. Ställning bör tas till hur detta arbete ska integreras i det riskanalysarbete som pågår inom ramen för FISK.

Informationens skyddsvärde bör beaktas med hjälp av klassningar, rapporterade incidenter och uppföljningar. Personer med ansvar och kunskap avseende informationssäkerhet bör i högre utsträckning involveras i arbetet med riskanalys.

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. 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 har visat att det ej förekommer dokumenterade kontrollåtgärder. Dokumenterade rutinbeskrivningar som är viktiga för kontroll och styrning av informationssäkerhet saknas i stor utsträckning.

Rutiner för behörigheter är en förutsättning för ett systematiskt arbete med att tilldela, ändra, ta bort och följa upp behörigheter. Granskningen har visat att dokumenterade rutiner för hantering av behörigheter saknas. Dokumenterade rutiner för hantering av privilegierade behörigheter för databaser, operativsystem mm saknas. Det görs ingen regelbunden eller dokumenterad uppföljning av privilegierade behörigheter, vilket är förenat med risker för hela myndigheten.

Granskningen visade att VXU saknar dokumenterade och fastställda kontinuitets-/avbrottsplaner för de gemensamma administrativa systemen som anger återställningstider, reservplaner vid avbrott, rutiner för återstart, krav på säkerhetskopiering, återläsningstester etc. Granskningen visade dock att det på central nivå genomförs dagliga säkerhetskopieringar. Det fanns dock inte kunskap på ledningsnivå om detta även görs på institutionsnivå. Kontroller av att säkerhetskopiorna går att återställa bör göras.

Förvaltningsplaner har bland annat som syfte att åstadkomma en systematisk plan för förvaltning av de olika systemen. Aktuella förvaltningsplaner som följer en beslutad modell är en förutsättning för att åstadkomma en systematisk förvaltning. VXU har inte en beslutad modell för förvaltning av systemen.

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

Förvaltningsmodell bör fastställas och förvaltningsplaner bör upprättas.

4.4. Information och kommunikation

En förutsättning för intern styrning och kontroll är att ledningen ger ett tydligt budskap om mål, risker, ansvar, befogenheter och rutiner.

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

4.5. 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.

I anslutning till att årsredovisningen skrivs under ska också styrelsen lämna en bedömning av huruvida den interna styrningen och kontrollen varit betryggande under året. Om informationssäkerhetsfrågor inte fullt ut beaktas i arbetet med FISK finns risk för att ledningens underlag för bedömningen av den interna styrningen och kontrollen inte är tillförlitligt.

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 VXU finns en utsedd person som ansvarar för IT-säkerheten, dock inte informationssäkerheten och uppföljning av denna. Någon plan för granskningar och åtgärder fanns inte vid granskningstillfället och det har inte heller framkommit att någon sådan dokumentation finns.

Riksrevisionens granskning visar att det inte förekommer några systematiska uppföljningar av informationssäkerheten varken från ledningsnivå eller på institutionsnivå.

Riksrevisionen *rekommenderar* att informationssäkerheten följs upp på ett systematiskt sätt, utifrån genomförda riskanalyser och kontrollåtgärder. En sammanställd redovisning av genomförda uppföljningar bör redovisas till styrelsen, som i anslutning till underskriften i årsredovisningen ska lämna en bedömning av huruvida den interna styrningen och kontrollen är betryggande.

Ansvarig revisor Christina Fröderberg har beslutat i detta ärende.
Uppdragsledare Nenus Jidah har varit föredragande.

Christina Fröderberg

Nenus Jidah

Kopia för kännedom:

Regeringen