Kungl. Konsthögskolan
Box 163 65
103 26 Stockholm

Datum 2011-03-09
Dnr 32-2010-0732

Granskning av intern styrning och kontroll av informationssäkerheten vid Kungl. Konsthögskolan 2010

Riksrevisionen har som ett led i den årliga revisionen granskat Kung. konsthögskolans (KKH) interna styrning och kontroll av informationssäkerhet.

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

Riksrevisionen önskar information senast 2011-06-15 med anledning av våra iakttagelser i denna rapport.

Sammanfattning

Mot bakgrund av det ökande elektroniska informationsutbytet i samhället har myndigheter under regeringen numera krav på sig utifrån Myndigheten för samhällskydd och beredskaps (MSB) föreskrifter och allmänna råd att tillämpa ett systematiskt arbete med informationssäkerhet utifrån etablerad svensk standard. Myndigheterna ska tillämpa ett så kallat ledningssystem för informationssäkerhet (LIS).

Riksrevisionen har under 2010 som ett led i den årliga revisionen granskat hur KKH 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. KKH har i samband med att högskolan fick möjlighet att faktagranska innehållet i denna rapport meddelat att styrelsen har beslutat om en ”Handbok för informations- och IT-säkerhet”.

Information är en av de viktigaste tillgångarna vid en myndighet. Oavsett vilken form informationen har och på vilket sätt den överförs eller lagras, måste den alltid ha godtagbart 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 är därför beroende av en god informationssäkerhet.

Riksrevisionens granskning visar att högskolan har delar av ett ramverk för styrning av informationssäkerheten. Det saknas dock fortfarande riktlinjer för att ramverket ska motsvara en etablerad standard. KKH behöver färdigställa den IT- och informationssäkerhetspolicy som högskolan arbetar med och dokumentera riktlinjer för bland annat behörighetsadministration, informationsklassning, kontinuitetsplanering och incidentövervakning. Befintlig riskanalys bör

kompletteras med mera informationssäkerhet. Det finns heller inte någon utsedd person som ansvarar för arbetet med informationssäkerhet vid KKH. Avtal med externa leverantörer bör kompletteras med en revisionsklausul.

1. Inledning

Intern styrning och kontroll förutsätter en god informationssäkerhet. Utan god informationssäkerhet finns det alltid betydande risker för informationens riktighet, sekretess, tillgänglighet och spårbarhet. Brister i ledningens upprättande och genomförande av generella kontroller för att uppnå en god informationssäkerhet kan medföra att myndighetens interna styrning och kontroll försvagas.

2. Normgivande regelverk

De normer som Riksrevisionen använt sig av vid bedömningen är

- Högskoleförordningen 2003:100
- Förordning (2006:942) om krisberedskap och höjd beredskap (krisberedskapsförordningen)
- Myndigheten för samhällsskydd och beredskaps föreskrifter (2009:10) om statliga myndigheters informationssäkerhet (MSB:s föreskrifter)
- Myndigheten för samhällsskydd och beredskaps allmänna råd (2009:10) till föreskrift om statliga myndigheters informationssäkerhet (MSB:s allmänna råd).

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.

I enlighet med 30 a § krisberedskapsförordningen ska varje myndighet ansvara för att myndighetens informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

Av 4 § MSB:s föreskrifter framgår att en myndighet i sitt arbete för en säker informationshantering ska tillämpa ett LIS. Det innebär bland annat att myndigheten ska upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. Myndigheten ska också utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet samt klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet. Utifrån risk- och sårbarhetsanalyser och inträffade incidenter ska avgöras hur risker ska hanteras samt beslut tas om åtgärder för myndighetens informationssäkerhet. Dokumentation krävs av de granskningar och säkerhetsåtgärder av större betydelse som har gjorts av myndigheten.

Av 5 § MSB:s föreskrifter framgår att myndighetens ledning löpande ska informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerheten på myndigheten.

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 samt på vilket sätt den överförs eller lagras måste den alltid ha ett godtagbart skydd.

3. Iakttagelser och rekommendationer

3.1 Otydligt vem som ansvarar för informationssäkerheten

LIS innebär bland annat att myndighetens ledning ska utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet. Det framgår indirekt av högskolans allmänna delegation att det är förvaltningschefen som har ansvaret för informationssäkerheten på KKH. KKH arbetar i dagsläget främst med IT-säkerhet. Riksrevisionen har inte uppfattat att det är någon som har ett uttalat, dokumenterat ansvar för informationssäkerheten.

Risken med att ansvaret för informationssäkerheten inte är tydligt utpekat är att det kan leda till att frågor rörande informationssäkerhet inte uppmärksammas i tillräcklig utsträckning. Det kan även leda till att högskolan har svårt att få en helhetsbild av risker och åtgärder, vilket kan försämra förutsättningarna för uppföljning. Det kan exempelvis vara svårt att samla och framföra en effektiv rapportering avseende informationssäkerhet till högskolans ledning.

Riksrevisionen *rekommenderar* KKH att förtydliga ansvaret för informationssäkerheten genom att ledningen utser någon att ansvara för området. Ansvaret bör dokumenteras samt specificeras i en arbetsbeskrivning. Ansvaret bör även kopplas till uppföljning av frågorna.

3.2 Regler för informationssäkerhet behöver dokumenteras

Enligt MSB:s föreskrifter ska myndigheten upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. KKH var under granskningstillfället i färd med att sammanställa en policy avseende IT- och informationssäkerhet. Vid granskningen noterades att det saknades riktlinjer kring behörighetsadministration, informationsklassning, incident- och problemhantering, programförändringar, mobiltelefoni, distansarbete samt för drift- och kontinuitetsplanering. För närvarande kommuniceras innehållet i de existerande styrdokumenten till stor del muntligen eftersom KKH bedömt att detta är mest effektivt.

Eftersom högskolan saknar dokumenterad styrning för flera viktiga områden medför detta en otydlighet som ökar risken för oönskad hantering av informationstillgångar med möjlig skada för KKH som följd.

Riksrevisionen *rekommenderar* KKH att färdigställa IT- och informationssäkerhetspolicyn samt upprätta övriga styrande dokument som reglerar hur information ska hanteras vid högskolan. De styrande dokumenten bör anpassas till KKH:s verksamhet. Styrdokumenten bör hållas tillgängliga så att medarbetare och elever enkelt och löpande kan ta del av dem.

3.3 Riskanalys och åtgärdsplan inte färdigställd

MSB anger i sina föreskrifter att myndigheten utifrån en risk- och sårbarhetsanalys ska avgöra hur risker ska hanteras samt besluta om åtgärder för myndighetens informationssäkerhet. KKH har en riskanalys som upprättades 2005, vilken behandlar bland annat IT-säkerhet men inte i egentlig mening behandlar informationssäkerhet. Under granskningstillfället pågick ett arbete med att upprätta en riskanalys som enligt plan ska vara riktad mot informationssäkerhet. Det finns dock ingen handlingsplan för hur högskolan ska åtgärda brister inom informationssäkerheten, vilket är en naturlig följd av att bristerna inte har analyserats.

Eftersom högskolan inte genomfört någon fullständig riskanalys avseende informationssäkerhet kan det försvåra för högskolan att identifiera vilka risker som föreligger. Det blir också svårare att bedöma sannolikheten för att det som bedöms riskfyllt inträffar och vilka konsekvenser en riskfylld händelse kan få för verksamheten. En låg medvetenhet om risker och deras konsekvenser kan i sin tur göra det svårt att avgöra vilka åtgärder som ska prioriteras. En väl genomförd riskanalys är nödvändig för att relevanta kontrollåtgärder och uppföljningsaktiviteter ska kunna utformas.

Riksrevisionen *rekommenderar* KKH att färdigställa en riskanalys som specifikt behandlar högskolans informationssäkerhet. För att den ska utgöra ett bra underlag för prioriteringar bör den omfatta sannolikheten för att en händelse inträffar samt vad konsekvensen av detta skulle bli. På detta sätt kan analysen ge ett bra underlag för hur riskerna bör prioriteras. Riskanalysen bör uppdateras regelbundet för att hållas aktuella. Eftersom miljön för de system som hanterar information förändras snabbt rekommenderar Riksrevisionen att uppdatering görs så snart förändringar sker. Utifrån riskanalysen bör högskolan sedan upprätta en handlingsplan med åtgärder och tidpunkter för när åtgärderna ska vidtas.

3.4 Rutin för hantering och övervakning av incidenter saknas

MSB skriver i sina allmänna råd att rutiner för incidentrapportering bör finnas. Rutinerna bör även säkerställa att incidenter utreds och hanteras. KKH har informella rutiner för att rapportera vissa typer av incidenter, bland dem kan nämnas förlust av datorer. Incidenter i högskolans IT-miljö tecknas ned när de inträffar för att man ska kunna lokalisera eventuella mönster i det som sker, men de inträffade incidenterna klassificeras/nivåindelas inte. KKH saknar dokumenterade rutiner för incidentrapportering.

KKH har inte någon formaliserad incidentrapportering vilket kan leda till att det tar längre tid att upptäcka och ta hand om problem. Det är svårare att avgöra vem som ska kontaktas eller vilka åtgärder som bör vidtas när incidenterna inte vare sig klassificeras eller nivåindelas. Det behövs även riktlinjer för när ledningen i olika nivåer ska informeras, en så kallad eskaleringsprocess.

Riksrevisionen *rekommenderar* KKH att upprätta rutiner för övervakning och hantering av incidenter. Rutinerna bör omfatta samtliga typer av incidenter som kan tänkas uppstå och som påverkar hanteringen av högskolans information**.** Incidenterna bör även klassificeras/nivåindelas. Riksrevisionen anser också att en eskaleringsprocess bör kopplas till incidentrapporteringen eftersom det är viktigt för att incidenter ska hanteras på rätt sätt så snart som möjligt efter att de inträffat. Genom att kontinuerligt följa upp incidenter kan KKH förhindra att de återkommer eller föranleder ytterligare skada. Samtliga rutiner bör dokumenteras eftersom det gör dem tydligare och lättare att kommunicera.

3.5 Dokumenterad kontinuitetsplanering saknas

MSB anger att kontinuitetsplaner för informationsförsörjningen bör upprättas och införas för att säkerställa att verksamheten ska kunna bedrivas enligt den nivå som beslutats efter genomförd riskanalys. KKH har upprättat en generell krisplan men har inte upprättat någon kontinuitetsplanering. Det finns inte heller någon upprättad avbrotts-/återstartsplan för högskolans system.

I och med att kontinuitetsplanering saknas löper högskolan risken att behoven för att upprätthålla kontinuitet i verksamheten inte kan värderas och tillgodoses. Eftersom det saknas en återstartsplan medför det att det blir svårare att göra avvägda prioriteringar vid en eventuell nedgång i system. Detta kan leda till förlust av information och förhindra effektivitet i återstartsprocessen.

Riksrevisionen *rekommenderar* KKH att upprätta och dokumentera en kontinuitetsplanering. Denna bör innefatta en återstartsplan där verksamhetskritiska system prioriteras. På detta sätt kan högskolan öka möjligheten att hantera eventuella nedgångar i systemen på ett effektivt sätt.

3.6 Revisionsklausul i avtal med externa leverantörer saknas

MSB:s allmänna råd anger att en myndighet som behöver samverka i fråga om informationssäkerhet kan överlåta till en annan myndighet att helt eller delvis fullgöra de uppgifter som åligger myndigheten. Detta ändrar dock inte högskolans ansvar för den egna informationssäkerheten. Högskolan använder sig av extern drift när det gäller Agresso. Enlig en bilaga till avtalet med ESVom Agresso Driftservice ingår bland annat följande tjänster när det gäller den tekniska plattformen: skalskydd, uppgradering av programvara, säkerhetskopiering, datalagring och arkivering av tape off-site, loggning samt behandlingshistorik. ESV svarar även för administrationen för användare och behörigheter för tillgång till Agressodriftens tjänster. KKH har inte fått information eller informerat sig om status eller gällande nivåer för dessa tjänster i och med att nuvarande avtal inte medger det.

Ledningen för den myndighet som uppdrar till annan myndighet att fullgöra uppgifter i fråga om informationssäkerhet bör löpande följa upp och informera sig om arbetet med informationssäkerhet på samma sätt som om uppgiften utförts av egen personal på myndigheten. Exempel på information är behörighetslistor, leverantörens rutiner för säkerhetskopiering, rapporter om återläsningstester av backuper och leverantörens systemförändringar.

Riksrevisionen *rekommenderar* KKH att verka för att få in en klausul i avtalet med externa leverantörer, till exempel avtalet avseende Agresso Driftservice, om revisionsrättigheter samt att myndigheten får tillgång till den information som rör högskolans verksamhet. Det är viktigt att det finns en klausul i avtalet om revisionsrättigheter som garanterar möjlighet till revision och utredning för till exempel externa revisorer, internrevisionen, säkerhetsbesiktningar av tredje part osv.

Ansvarig revisor Carin Rytoft Drangel har beslutat i detta ärende.
Medverkande revisor Christian Armandt har varit föredragande.

Carin Rytoft Drangel Christian Armandt

Kopia för kännedom:

Regeringen
Utbildningsdepartementet
Finansdepartementet (budgetavdelningen)