Dans- och cirkushögskolan
Box 27043
102 51 Stockholm

Datum 2011-03-08
Dnr 32-2010-0726

Granskning av intern styrning och kontroll av informationssäkerheten vid Dans- och cirkushögskolan 2010

Riksrevisionen har som ett led i den årliga revisionen granskat Dans- och cirkushögskolans (DOCH) interna styrning och kontroll av informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa DOCH: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 DOCH 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.

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. Det finns inte någon utsedd person som ansvarar för arbetet med informationssäkerhet vid DOCH. Dokumenterade riktlinjer för behörighetsadministration och incidentövervakning behöver upprättas. Befintlig risk- och åtgärdsplan bör kompletteras med informationssäkerhet. 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 föreskrift 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. Förvaltningschefen har i dag genom delegation från rektor ansvaret för säkerheten vid högskolan. Eftersom detta avser den totala säkerheten, inklusive IT-säkerheten, är det ett brett definierat ansvar. Viss del av ansvaret är vidaredelegerat till säkerhets- och teknikansvarig genom högskolans för delningsordning. Riksrevisionen har inte uppfattat att det är någon som har ett utpekat samt 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 informationssäkerheten till högskolans ledning.

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

3.2 Regler för informationssäkerhet saknas

Enligt MSB:s föreskrifter ska myndigheten upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. DOCH hade vid granskningen inte någon upprättad policy för informationssäkerhet. Vid granskningen noterades att det saknades flera styrande dokument, till exempel riktlinjer för klassning av information. Riksrevisionen har efter granskningstillfället erhållit ett utkast till informationssäkerhetspolicy.

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 DOCH som följd.

Riksrevisionen *rekommenderar* DOCH att besluta om en informationssäkerhetspolicy samt upprätta övriga styrande dokument som reglerar hur information ska hanteras vid högskolan. De styrande dokumenten bör anpassas till DOCH:s verksamhet. Högskolan bör sedan avgöra hur de på effektivast möjliga sätt kommunicerar riktlinjerna för informationshanteringen. Styrdokumenten bör hållas tillgängliga så att medarbetare och elever enkelt och löpande kan ta del av dem.

3.3 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. DOCH har informella rutiner för hantering av vissa typer av incidenter, bland dem kan nämnas förlust av datorer och telefoner. Rutinerna är inte formaliserade eller

dokumenterade och det finns ingen samlad rutin för loggning och rapportering av incidenter.

Eftersom DOCH inte har någon formaliserad incidentrapportering kan detta 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 vare sig klassificeras eller nivåindelas. Det behövs även riktlinjer för när ledningen i olika nivåer ska informeras, en så kallad eskaleringsprocess. Eftersom incidenter inte dokumenteras i en logglista för uppföljning, har högskolan mindre möjligheter att upptäcka återkommande problem och lära sig av dessa.

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

3.4 Riskanalys och åtgärdsplan bör kompletteras med informationssäkerhet

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. DOCH arbetar i dag med riskanalyser inom vissa områden. Riskanalyserna uppdateras enligt plan vart femte år även om det finns planer på att göra detta oftare. Högskolan har inte upprättat någon riskanalys som direkt behandlar informationssäkerheten. Det finns inte heller någon åtgärdsplan för hur högskolan ska åtgärda brister inom informationssäkerheten.

Eftersom högskolan inte genomfört några riskanalyser avseende informationssäkerheten 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. Om riskanalysen inte uppdateras vid förändringar löper den risken att inte vara ändamålsenlig, eftersom den måste möta kontinuerliga och snabba förändringar i informationsmiljön. En väl genomförd riskanalys är nödvändig för att relevanta kontrollåtgärder och uppföljningsaktiviteter ska kunna utformas.

Riksrevisionen *rekommenderar* DOCH att upprätta 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 kontinuerligt för att hållas aktuell. Eftersom miljön för de system som hanterar information förändras snabbt rekommenderas att uppdateringar sker vid

förändringar. Utifrån riskanalyserna bör högskolan sedan upprätta en åtgärdsplan med åtgärder och tidpunkter för när åtgärderna ska vidtas.

3.5 Formalisera och dokumentera rutin för behörighetsadministration

MSB föreskriver i sina allmänna råd att övergripande riktlinjer för åtkomst- och behörighetsstyrning bör upprättas som en del av regelverket för informationssäkerhet. DOCH har vissa rutiner avseende behörighetsadministration men de är inte formaliserade eller dokumenterade.

Högskolan saknar formaliserade och dokumenterade rutiner för tillägg, ändring, borttagande och uppföljning av behörigheter till nätverk, applikationer eller systemresurser. Detta kan medföra en risk för obehörig åtkomst till information eller program, med läckage eller förlust av information samt eventuellt brister i spårbarhet som följd.

Riksrevisionen *rekommenderar* DOCH att införa dokumenterade rutiner för hantering (tilldelning, ändring, borttagande och uppföljning) av behörigheter. Högskolan behöver också fastställa rutiner för privilegierade behörigheter för databaser, operativsystem m.m. Rutiner för hantering av behörigheter är nödvändiga för att kontinuerligt försäkra sig om att ingen har högre behörighet än vad som krävs utifrån arbetsuppgiften och för att säkerställa informationens integritet. Dokumentationen bör även beskriva med vilka intervall periodisk uppföljning av befintliga behörigheter ska ske samt ge riktlinjer för tillfälliga behörigheter.

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. Enligt bilaga till avtalet med ESV om 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. För ett stort antal övriga system tillhandahålls driftservice av KTH. DOCH har inte kravställt eller fått dokumentation om exempelvis nivån på leverantörens åtgärder för att behålla kontinuiteten.

Ledningen för den myndighet som uppdrar till annan 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* DOCH 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)