Konstfack
Box 3601
126 27 Stockholm

Datum 2011-03-09
Dnr 32-2010-0731

Granskning av intern styrning och kontroll av informationssäkerheten vid Konstfack 2010

Riksrevisionen har som ett led i den årliga revisionen granskat Konstfacks (KF) interna styrning och kontroll av informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa KF:s uppmärksamhet på i denna revisionsrapport. KF har ett decentraliserat system för informationssäkerheten där riktlinjer har utvecklats olika för olika system. De iakttagelser som lämnas i rapporten avser övergripande riktlinjer och dokumentation avseende informationssäkerheten hos KF.

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 KF 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 KF har ett decentraliserat system för informationssäkerheten där riktlinjer har utvecklats olika för olika system. KF har påbörjat ett arbete med att centralisera sin IT-organisation. De iakttagelser som lämnas i rapporten avser övergripande riktlinjer och dokumentation avseende informationssäkerheten hos KF. Det finns inte någon utsedd person som ansvarar för arbetet med informationssäkerhet vid KF. KF behöver fastställa sitt utkast till policy för informationssäkerhet. Dokumenterade riktlinjer för behörighetsadministration, kontinuitetsplaner, incidentövervakning

samt informationsklassning behöver upprättas. KF behöver upprätta en riskanalys som behandlar informationssäkerheten. Avtal med externa leverantörer bör kompletteras med en revisionsklausul. KF bör överväga att förvara säkerhetskopior på en geografisk plats som är skild från originaldata och även regelbundet testa om säkerhetskopiorna går att återläsa.

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. KF har inget dokumenterat beslut som delegerar ansvaret.

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 det blir 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* KF 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 behöver dokumenteras

Enligt MSB:s föreskrifter ska myndigheten upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. KF hade vid granskningen upprättat ett utkast till en policy för informationssäkerhet. Policyn var inte formellt beslutad. Vid granskningen noterades att det saknades flera styrande dokument till exempel avseende behörighetsadministration, informationsklassning, rutiner för incident- och problemhantering, rutiner för programförändringar samt drift- och kontinuitetsplanering.

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 KF som följd.

Riksrevisionen *rekommenderar* KF att fastställa sin informationssäkerhetspolicy samt upprätta övriga styrande dokument som reglerar hur information ska hanteras vid högskolan. De styrande dokumenten bör anpassas till KF:s verksamhet. KF bör sedan avgöra hur högskolan 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 behörighetsadministration saknas

MSB föreskriver i sina allmänna råd att övergripande riktlinjer för åtkomst- och behörighetsstyrning bör upprättas som en del av regelverket för informationssäkerhet. KF har vissa rutiner avseende behörighetsadministration, men de är inte formaliserade eller dokumenterade. Rutinerna skiljer sig mellan olika system vid högskolan. KF:s IT-policy föreskriver att lösenord ska utformas efter vissa komplexitetskrav men dessa är inte tvingande och kraven följs inte genomgående.

Myndigheten 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. Eftersom krav på lösenord inte följs ökar risken för att lösenord avslöjas eller manipuleras.

Riksrevisionen *rekommenderar* KF 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.

3.4 Riskanalys och åtgärdsplan saknas

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. KF har inte upprättat någon riskanalys som behandlar informationssäkerheten vid högskolan. Det finns heller ingen åtgärdsplan för hur högskolan ska åtgärda brister inom området.

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. En väl genomförd riskanalys är nödvändig för att relevanta kontrollåtgärder och uppföljningsaktiviteter ska kunna utformas.

Riksrevisionen *rekommenderar* KF att upprätta en riskanalys som 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 uppdatering sker vid förändringar. Utifrån riskanalyserna bör högskolan sedan upprätta en åtgärdsplan med åtgärder och tidpunkter för när åtgärderna ska vidtas.

3.5 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. KF har informella rutiner för hantering av vissa typer av incidenter. Rutinerna är inte formaliserade eller dokumenterade och det finns ingen samlad rutin för loggning och rapportering av incidenter.

KF 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. Eftersom incidenter inte dokumenteras i en logglista för uppföljning har högskolan mindre möjligheter att upptäcka återkommande problem och lära sig av dessa.

Riksrevisionen *rekommenderar* KF 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 så snart som möjligt efter att de inträffat. Genom att kontinuerligt följa upp incidenter kan KF förhindra att de återkommer eller föranleder ytterligare skada. Samtliga rutiner bör dokumenteras eftersom det gör dem tydligare och lättare att kommunicera.

3.6 Rutiner för återläsningstest av säkerhetskopierad data saknas

MSB skriver i sina allmänna råd att rutiner för incidenthantering bör finnas för att mildra effekter av händelser samt underlätta återgång till normal drift. För att säkerställa att kontinuiteten i verksamheten upprätthålls krävs att det finns en betryggande säkerhetskopiering. KF säkerhetskopierar de data som finns i de olika systemen men gör inga återläsningstester av säkerhetskopierad data. Säkerhetskopierad data förvaras i samma lokal som originaldatan.

Eftersom original och kopior förvaras i samma lokal kommer en fysisk incident i form av brand, vattenläcka eller dylikt sannolikt att påverka både original och kopior. KF löper ytterligare risk för att säkerhetskopiorna inte är intakta eftersom högskolan inte genomför några återläsningstester av den sparade informationen.

Riksrevisionen *rekommenderar* KF att förvara säkerhetskopior på en geografisk plats som är skild från originaldata. KF bör även regelbundet testa om säkerhetskopiorna går att återläsa.

3.7 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. KF har inte upprättat någon kontinuitetsplanering. Det finns inte heller någon samlad 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. Avsaknaden av en återstartsplan medför 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* KF 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.

3.8 Upprätta riktlinjer för klassning av information

MSB:s föreskrifter anger att myndigheten ska klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet. KF har inte något system för klassning av information.

Risken med att inte göra någon klassning av information är att det blir svårare att arbeta preventivt för att skydda informationen. Utan kunskap om hur informationen ska klassas blir det svårare att veta vilken skyddsnivå den bör ha. Detta kan medföra att känslig information inte får det skydd den behöver och att det läggs för mycket resurser på att skydda förhållandevis okänslig information.

Riksrevisionen *rekommenderar* KF att upprätta riktlinjer för hur högskolan klassificerar olika typer av information. För att på ett effektivt sätt kunna avgöra hur kritisk informationen är och vilket skydd den är i behov av bör någon form av klassning av informationen göras redan när den kommer till eller upprättas vid myndigheten. Klassningen bör vara kopplad till myndighetens riskanalys.

3.9 Centralisera ansvar för IT

För att ha en god intern styrning och kontroll avseende sin IT-miljö krävs en överblick över IT-miljön. Miljön bör vara ensad och integrerad i högsta möjliga mån. Det underlättar även att hålla rutiner och riktlinjer enhetliga. KF har decentraliserat och fördelat ansvaret för sin IT-miljö mellan olika enheter inom högskolan. Detta innebär att det finns ett antal olika ansvariga medarbetare och förhållandevis många olika lösningar i IT-miljön. KF planerar att centralisera IT-organisationen under 2011.

Risken med att sprida ansvaret för IT-miljön är att det kan bli svårt att få en helhetsbild av miljön samt för risker och brister i den. Det kan också generera att KF tvingas arbeta med ett antal olika lösningar vad gäller tekniska lösningar och rutiner. Detta kan medföra att det blir svårt att skapa en enhetlig IT-miljö, vilket i sin tur kan göra den känslig. Det kan bland annat leda till att arbetet inte genomförs effektivt. Utöver detta försvårar det kommunikation av rutiner och policyer eftersom arbete bedrivs olika inom olika delar av organisationen.

Riksrevisionen *rekommenderar* KF att fullfölja sin plan att centralisera sin IT-organisation. På detta sätt kommer högskolan att skapa förutsättningar för en enhetlig IT-miljö. Detta kommer i sin tur att effektivisera arbetet och göra miljön mindre sårbar. Avslutningsvis kommer det sannolikt även att förenkla för högskolan att ha enhetliga rutiner inom organisationen.

3.10 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. KF 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* KF 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)