Gymnastik- och idrottshögskolan
Box 5626
114 86 Stockholm

Datum 2011-03-08
Dnr 32-2010-0728

Granskning av intern styrning och kontroll av informationssäkerheten vid Gymnastik- och idrottshögskolan 2010

Riksrevisionen har som ett led i den årliga revisionen granskat Gymnastik- och idrottshögskolans (GIH) interna styrning och kontroll av informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa GIH: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 GIH 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. Högskolans informationssäkerhetspolicy behöver kompletteras med flera viktiga aspekter av informationssäkerhetsarbete. GIH saknar även en rutin för uppföljning av informationssäkerhetsarbetet. Dokumenterade riktlinjer för behörighetsadministration, kontinuitetsplaner och incidentövervakning behöver upprättas. Befintlig riskanalys bör kompletteras med mera informationssäkerhet. Avtal med externa leverantörer bör kompletteras med en revisionsklausul. GIH

behöver regelbundet testa om den information högskolan får skickat till sig i form av bandkopior går att återläsa. GIH bör arbeta med att komma till rätta med det nyckelpersonsberoende som finns avseende IT-arbetet.

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 Rutin för uppföljning av informationssäkerhetsarbetet saknas

Ledningen ska enligt MSB:s föreskrifter löpande informera sig om arbetet med informationssäkerheten och minst en gång per år följa upp och utvärdera arbetet. Högskolan har planer på att arbetet med informationssäkerhet ska integreras i verksamhetsplaneringsarbetet. Under granskningstillfället hade GIH inte någon rutin för uppföljning av arbetet och den som är ansvarig för informationssäkerheten föredrar i nuläget inte arbetet för ledningen.

Risken med att det inte sker någon uppföljning av arbetet med informationssäkerheten är att ledningen inte får information om vilka brister som föreligger. Detta medför att de som är ytterst ansvariga för högskolans verksamhet får svårt att ta relevanta beslut för att komma till rätta med eventuella problem inom området. Ledningen ges heller inte några bra underlag för utvärdering av det arbete som utförs. Detta medför i sin tur att de inte kan avgöra vad resultatet av vidtagna åtgärderna är.

Riksrevisionen *rekommenderar* GIH att upprätta rutiner för regelbunden uppföljning av arbetet med informationssäkerhet. Rutinerna bör säkerställa att ledningen vid högskolan hålls uppdaterade om vilka risker som föreligger avseende informationssäkerheten. Om GIH väljer att integrera arbetet med informationssäkerheten i verksamhetsplaneringen är det viktigt att samtliga delar av högskolans verksamhet ges uppmärksamhet. För att följa upp att beslutade åtgärder vidtas och avgöra om arbetet bedrivs på ett tillfredställande sätt bör ledningen även följa upp och utvärdera arbetet.

3.2 Rutin för behörighetsadministration behöver dokumenteras

MSB föreskriver i sina allmänna råd att övergripande riktlinjer för åtkomst- och behörighetsstyrning bör upprättas som en del av regelverket för informationssäkerhet. GIH 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* GIH 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.

3.3 Dokument avseende informationssäkerhet behöver kompletteras och kommuniceras

Enligt MSB:s föreskrifter ska myndigheten upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. GIH hade vid granskningen en informationssäkerhetspolicy. Policyn var väldigt övergripande och behöver kompletteras med avseende på informationsklassning, incident- och problemhantering, behörighetsadministration, programförändringar samt drift- och kontinuitetsplanering. GIH håller en introduktionsutbildning för nyanställda på myndigheten. Introduktionsutbildningen används inte för att informera om informationssäkerhet.

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 GIH som följd. Eftersom introduktionsutbildningen inte används för att informera om informationssäkerhet medför det risk att personalen inte får tillräcklig kunskap om gällande regler.

Riksrevisionen *rekommenderar* GIH att komplettera informationssäkerhetspolicyn med flera viktiga aspekter av informationssäkerhet samt upprätta övriga styrande dokument som reglerar hur information ska hanteras vid högskolan. De styrande dokumenten bör anpassas till GIH:s verksamhet. GIH bör sedan avgöra hur högskolan på effektivast möjliga sätt kommunicerar riktlinjerna för informationshanteringen. GIH bör ta upp informationssäkerhet i sin introduktionsutbildning.

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. GIH arbetar i dag med riskanalyser inom vissa områden. Riskanalyserna uppdateras enligt plan vart femte år. 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 någon 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. 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* GIH 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 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. GIH har informella rutiner för hantering av vissa typer av incidenter. De är inte formaliserade eller dokumenterade och det finns ingen samlad rutin för loggning och rapportering av incidenter. Det finns en informell gång för eskalering av incidenter men det saknas formella riktlinjer för när incidenter ska rapporteras till ledningen på olika nivåer, en så kallad eskaleringsprocess.

GIH 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 vare sig klassificeras eller nivåindelas. Det behövs även en 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* GIH 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 GIH förhindra att de återkommer eller föranleder ytterligare skada. Samtliga rutiner bör dokumenteras eftersom det gör dem tydligare och lättare att kommunicera.

3.6 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. GIH har inte upprättat någon kontinuitetsplanering för myndigheten. 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. 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* GIH 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.

3.7 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. GIH:s IT-leverantör skickar regelbundet bandkopior till högskolan innehållande backup. Banden förvaras i brandskyddade skåp på högskolan. GIH har inte någon utrustning för att återläsa backuperna.

Avsaknad av utrustning för att kunna återläsa erhållna bandkopior medför risk att GIH inte kan säkerställa att backuperna högskolan får av leverantören är användbara.

Riksrevisionen *rekommenderar* GIH att regelbundet testa om den information högskolan får skickat till sig i form av bandkopior går att återläsa.

3.8 Minska nyckelpersonsberoende kring IT-miljön

Styrelsen vid GIH har i enlighet med 2 § i högskoleförordningen ansvar för att säkerställa att det vid högskolan finns en intern styrning och kontroll som fungerar på ett betryggande sätt. En aspekt av detta är att se till att kunskap som är kritisk för verksamheten finns att tillgå. På GIH finns i dag en person som huvudsakligen sköter IT-arbetet på högskolan.

Eftersom i huvudsak en person sköter IT-miljön på högskolan föreligger ett nyckelpersonsberoende. Detta kan innebära att högskolan får stora problem vid händelse av att medarbetaren slutar eller av annan anledning inte finns tillgänglig för att sköta driften av IT-miljön.

Riksrevisionen *rekommenderar* GIH att arbeta med att komma till rätta med nyckelpersonsberoendet. En åtgärd är att kunskapsöverföra kompetens till medarbetare inom myndigheten kring de mest verksamhetskritiska arbetsmomenten. Ytterligare en insats för att motverka problematiken skulle vara att upprätta skriftliga arbetsbeskrivningar över IT-teknikerns arbetsmoment.

3.9 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. GIH 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 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* GIH 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)