Högskoleverket
Box 7851
103 99 Stockholm

Datum 2011-03-08
Dnr 32-2010-0730

Granskning av intern styrning och kontroll av informationssäkerheten vid Högskoleverket 2010

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

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa HSV: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 HSV 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 myndigheten har delar av ett ramverk för styrning av informationssäkerheten. Befintliga informationssäkerhetsinstruktioner för förvaltning samt kontinuitet och drift behöver dock kompletteras med en samlad informationssäkerhetspolicy för att i motsvara etablerad standard. HSV bör även fullfölja det påbörjade arbetet med informationsklassning samt upprätta riktlinjer för hur HSV klassificerar olika typer av information. Dokumenterade riktlinjer för behörighetsadministration och kontinuitetsplanering behöver upprättas. Befintlig riskanalys bör kompletteras med flera viktiga aspekter av informationssäkerhet. Dessutom finns inte någon utsedd person som ansvarar för arbetet med informationssäkerhet vid HSV. Formaliserade och dokumenterade förvaltningsmodeller kopplade till

den administrativa avdelningen saknas. HSV bör överväga att använda introduktionsutbildningarna till att informera om informationssäkerhet. HSV bör även överväga att förvara säkerhetskopior på en geografisk plats som är skild från originaldata.

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

- Myndighetsförordning (2007:515)
- Förordning (2006:942) om krisberedskap och höjd beredskap (krisberedskapsförordningen)
- Myndigheten för samhällskydd och beredskaps föreskrifter (2009:10) om statliga myndigheters informationssäkerhet (MSB:s föreskrifter)
- Myndigheten för samhällskydd och beredskaps allmänna råd (2009:10) till föreskrift om statliga myndigheters informationssäkerhet (MSB:s allmänna råd).

Av 4 § i myndighetsförordningen framgår att det är styrelsens ansvar att säkerställa att det vid myndigheten 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. I myndighetens arbetsordning framgår att administrativa avdelningen ansvarar för säkerhetsfrågor och att IT-avdelningen ansvarar för IT-säkerhetsfrågor. Riksrevisionen har inte uppfattat att det är någon som har ett utpekat 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 myndigheten 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 myndighetens ledning.

Riksrevisionen *rekommenderar* HSV 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 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. HSV har inte någon rutin för uppföljning av informationssäkerhetsarbetet, vilket innebär att arbetet i nuvarande situation inte föredras 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 myndighetens 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.

Riksrevisionen *rekommenderar* HSV att upprätta rutiner för regelbunden uppföljning av arbetet med informationssäkerhet. Rutinerna bör säkerställa att ledningen vid myndigheten hålls uppdaterade om vilka risker som föreligger avseende informationssäkerheten. För att följa upp att beslutade åtgärder vidtas och avgöra om arbetet bedrivs på ett tillfredställande sätt bör ledningen följa upp och utvärdera arbetet.

3.3 Rutin för behörighetsadministration saknas

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

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.

Riksrevisionen *rekommenderar* HSV att införa dokumenterade rutiner för hantering (tilldelning, ändring, borttagande och uppföljning) av behörigheter. Myndigheten behöver också dokumentera rutiner för höga behörigheter till 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 säkerhet. Dokumentationen bör även innehålla riktlinjer för tillfälliga behörigheter.

3.4 Fortsätt arbetet med riktlinjer för att hantera information beroende på hur den är klassificerad

MSB:s föreskrifter anger att myndigheten ska klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet. HSV har påbörjat ett arbete med informationsklassning där myndigheten har utgått från viktig information för organisationen ur perspektiven konfidentialitet, riktighet och sekretess. Arbetet är inte slutfört, eftersom all information ännu inte är kategoriserad.

Risken med att inte ha någon fullständig klassning av information är att det blir svårare att arbeta förebyggande 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* HSV att fullfölja det påbörjade arbetet med informationsklassning samt upprätta riktlinjer för hur myndigheten klassificerar olika typer av information. Klassningen bör vara kopplad till myndighetens riskanalys.

3.5 Riskanalys och åtgärdsplan bör kompletteras med mera 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. HSV har analyserat vissa områden, men någon heltäckande riskanalys avseende informationssäkerhet har inte genomförts. Riskanalysen bör omfatta alla typer av informationssäkerhetsrisker – bristande tillgänglighet, riktighet, sekretess och spårbarhet – som kan vara väsentliga i verksamheten. Det finns ingen heltäckande åtgärdsplan för hur HSV ska åtgärda brister inom informationssäkerheten.

Eftersom myndigheten inte genomför några riskanalyser som är direkt kopplade till informationssäkerheten kan det försvåra för myndigheten 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* HSV att upprätta en riskanalys som specifikt behandlar myndighetens informationssäkerhet. Eftersom myndigheten redan

har delar av en riskanalys är ett alternativ att en enskild analys upprättas för informationssäkerheten. Risker från denna kan sedan lyftas upp till myndighetens totala analys i den omfattning det bedöms relevant. Riskanalyserna 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 riskanalyserna bör HSV sedan upprätta en åtgärdsplan med åtgärder och tidpunkter för när åtgärderna ska vidtas.

3.6 Regler för informationssäkerhet behöver kompletteras

Enligt MSB:s föreskrifter ska myndigheten upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. HSV har upprättade informationssäkerhetsinstruktioner för förvaltning (Infosäk F) samt kontinuitet och drift (Infosäk KD). Infosäk KD är dock inte färdigställd. Vid granskningstillfället fanns ingen upprättad samlad informationssäkerhetspolicy, och den IT-policyn som finns fokuserar på arbetssättet och inte på säkerheten. Utöver dessa dokument finns ytterligare styrdokument som behandlar informationssäkerhet på olika ställen på HSV:s intranätet.

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

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

3.7 Förvaltningsmodell saknas för de administrativa systemen

MSB:s allmänna råd föreskriver att särskild uppmärksamhet bör läggas på att verksamhetens säkerhetskrav beaktas vid utveckling, anskaffning och avveckling av informationsbehandlingsresurser. Under granskningstillfället noterades att systemförvaltningen skilde sig åt beroende på IT-system. Formaliserade och dokumenterade förvaltningsmodeller för system kopplade till den administrativa avdelningen saknas.

Risken med att inte ha en tydlig förvaltningsmodell är att man inte uppnår kontroll av förvaltningsprocessen och att man inte får ut optimal nytta av informationssystemet. Risken finns också att rutiner inte skapas för förändringar i systemet samt att det är svårt att få en helhetsbild av systemförvaltningen.

Riksrevisionen *rekommenderar* HSV att upprätta förvaltningsmodeller för sina administrativa system enligt samma princip som myndighet använder för sina andra system.

3.8 Inkludera informationssäkerhet i introduktionsutbildningen

MSB:s allmänna råd anger att god informationssäkerhet förutsätter att all berörd personal känner till och medverkar till att gällande regelverk följs. Därför bör säkerhetsfrågor också vara en naturlig del i relationen mellan arbetsgivare och arbetstagare från anställningens början till dess att den upphör. HSV håller

en introduktionsutbildning för nyanställda på myndigheten. Introduktionsutbildningen innehåller ingen separat del om informationssäkerhet.

Avsaknaden av en separat del om informationssäkerhet på introduktionsutbildningen för de nyanställda medför risk att personalen inte får tillräcklig kunskap om gällande regler för informationssäkerhet.

Riksrevisionen *rekommenderar* HSV att införa ett separat avsnitt kring informationssäkerhet i sina introduktionsutbildningar.

3.9 Kontinuitetsplanering saknas

MSB:s allmänna råd 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. HSV har inte upprättat någon kontinuitetsplanering för myndigheten. Det finns inte heller någon upprättad avbrotts-/återstartsplan för myndighetens system.

I och med att kontinuitetsplanering saknas löper myndigheten 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* HSV att upprätta och dokumentera en kontinuitetsplanering. Denna bör innefatta en återstartsplan där verksamhetskritiska system prioriteras. På detta sätt kan myndigheten öka möjligheten att hantera eventuella nedgångar i systemen på ett effektivt sätt.

3.10 Se till att geografiskt separera backup från serverhall

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. HSV tar säkerhetsbackuper regelbundet men förvarar backuperna i samma lokal som originaldatan. HSV förvarar backuperna i säkerhetsskåp.

Eftersom original och kopior förvaras på samma geografiska plats kommer en fysisk incident i form av brand, vattenläcka eller dylikt sannolikt att påverka både original och kopior.

Riksrevisionen *rekommenderar* HSV att överväga att förvara säkerhetskopior på en geografisk plats som är skild från originaldata.

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)