Verket för högskoleservice
Box 24070
104 50 Stockholm

Datum 2011-03-08
Dnr 32-2010-0738

Granskning av intern styrning och kontroll av informationssäkerheten vid Verket för högskoleservice 2010

Riksrevisionen har som ett led i den årliga revisionen granskat Verket för högskoleservices (VHS) interna styrning och kontroll av informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa VHS 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 VHS 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. VHS befintliga IT-policy samt rutiner och riktlinjer för informationssäkerhet behöver dock uppdateras samt kompletteras med fler riktlinjer för att i större utsträckning motsvara etablerad standard. De rutiner som finns avseende behörighetsadministration och incidentövervakning behöver kompletteras samt dokumenteras. Dokumenterade riktlinjer för informationsklassning och incidentövervakning behöver upprättas. Befintlig riskanalys bör kompletteras med flera viktiga

aspekter av informationssäkerhet. VHS behöver även överväga ett förstärkt skydd vid uppkoppling för distansarbete. Dessutom finns inte någon utsedd person som ansvarar för arbetet med informationssäkerhet vid VHS.

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 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 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 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 att bland annat att myndighets ledning ska utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet. VHS hade vid granskningen planer på att utse någon som ansvarade för informationssäkerheten men hade ännu inte gjort det. Det fanns således inget formellt beslut som delegerar ansvaret och av det följer även att ansvaret inte finns dokumenterat.

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 informationssäkerhet till myndighetens ledning.

Riksrevisionen *rekommenderar* VHS att fullfölja arbetet med 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 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. VHS har upprättat riskanalyser för myndigheten som helhet. I denna behandlas vissa frågor med koppling till informationssäkerhet, men riskanalysen bör omfatta alla typer av informationssäkerhetsrisker – bristande tillgänglighet, riktighet, sekretess och spårbarhet – som kan vara väsentliga i verksamheten. I den analys som finns upprättad är risker värderade efter sannolikhet och konsekvens och det finns planerade åtgärder och utpekat ansvar för att minska flera av riskerna, dock inte samtliga. Ett exempel på risk utan planerad åtgärd är till exempel ”Risk föreligger att känslig eller hemlig information hanteras felaktigt och att skadlig spridning av sådan information kan ske”.

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* VHS att upprätta en riskanalys som specifikt behandlar myndighetens informationssäkerhet. Eftersom myndigheten redan har en rutin för upprättande av riskanalyser är ett alternativ att en enskild analys upprättas för informationssäkerheten. Risker från denna kan sedan lyftas upp i 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 VHS sedan upprätta en handlingsplan med åtgärder och tidpunkter för när åtgärderna ska vidtas för samtliga risker.

3.3 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. VHS 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* VHS att införa dokumenterade rutiner för hantering (tilldelning, ändring, borttagande och uppföljning) av behörigheter. Myndigheten 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 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. VHS 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* VHS att upprätta riktlinjer för hur myndigheten ska klassificera 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.

3.5 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. VHS har inte upprättat

någon kontinuitetsplanering. Myndigheten har inte heller avbrotts-/återstartsplaner för alla sina 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 återstartsplaner för vissa system medför att det blir svårare att göra avvägda prioriteringar vid en eventuell nedgång i systemen. Detta kan leda till förlust av information och förhindra effektivitet i återstartsprocessen.

Riksrevisionen *rekommenderar* VHS att upprätta och dokumentera en kontinuitetsplanering. I samband med detta bör myndigheten även upprätta återstartsplaner för samtliga system. Verksamhetskritiska system bör prioriteras i planen. Genom att genomföra dessa åtgärder kan VHS öka möjligheten att hantera eventuella nedgångar i systemen på ett effektivt sätt.

3.6 Se till att styrande dokument uppdateras regelbundet och samlas på intranätet

Enligt MSB:s föreskrifter ska myndigheten upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. VHS hade vid granskningen ett antal styrdokument, däribland en IT-policy samt rutiner och riktlinjer för IT-säkerhet. Dokumenten finns tillgängliga på intranätet men inte i samlad form. Dokumenten har inte uppdaterats på länge och VHS saknar rutiner för hur ofta de ska uppdateras.

Risken med att styrdokument inte uppdateras på regelbunden basis är att de kan tappa sin relevans och bli felaktiga. Om styrande dokument inte anpassas till förändringar i den miljö de är avsedda att styra kommer de inte att svara mot de problem som myndigheten ställs inför. Det kan även innebära att dokumenten inte uppdateras i takt med att myndigheten ändrar rutiner och arbetssätt. Detta medför att de som hanterar information vid myndigheten inte har tillgång till korrekta rutiner.

Riksrevisionen *rekommenderar* VHS att gå igenom sina styrdokument och uppdatera dem vid förändringar. Myndigheten bör även formalisera en rutin för regelbundna genomgångar av dem. På detta sätt kan myndigheten förhindra att dokumenten tappar sin relevans eller blir inaktuella. Styrdokumenten hålls med fördel tillgängliga via intranät eller liknande och då gärna i samlad form.

3.7 Förstärk skyddet vid uppkoppling för distansarbete

MSB:s allmänna råd föreskriver att alla förhållanden för drift av IT-system och datakommunikation bör beaktas från säkerhetssynpunkt. Rutinerna bör vara dokumenterade och även innefatta skydd av datamedia. Under granskningen framkom att vid uppkoppling mot VHS system vid distansarbete inte finns något krav på så kallad stark autentisering. Detta innebär att det krävs ytterligare en identifikation utöver inloggningen via klientprogrammet för dem som ska koppla upp sig mot myndighetens nätverk när de befinner sig på annan plats, till exempel en dosa att använda vid inloggning.

Risken med VHS lösning för distansarbete är att datakommunikationen mellan den distansarbetandes dator och myndighetens nätverk inte har ett tillfredsställande skydd. Att endast ha en faktor för identifiering gör nätverket

känsligare för angrepp. Detta förenklar intrång i VHS system med förvanskning, förstörelse och stöld av information som en möjlig följd.

Riksrevisionen *rekommenderar* VHS att överväga krav på stark autentisering för distansarbete både för sina interna medarbetare samt även för sina externa konsulter. Genom att införa sådana rutiner minskar VHS risken för otillbörliga intrång i nätverket.

3.8 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. VHS 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.

VHS har inte någon formaliserad och samlad 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 riktlinjer för när ledningen i olika nivåer ska informeras, en så kallad eskaleringsprocess. Eftersom incidenter inte loggas har myndigheten mindre möjligheter att upptäcka återkommande problem och lära sig av dessa.

Riksrevisionen *rekommenderar* VHS att upprätta en samlad rutin för övervakning, loggning och hantering av incidenter. Rutinerna bör omfatta samtliga typer av incidenter som kan tänkas uppstå och påverkar hanteringen av myndighetens 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 och så snart som möjligt efter att de inträffat. Genom att kontinuerligt följa upp incidenter kan VHS förhindra att de återkommer eller föranleder ytterligare skada. Samtliga rutiner bör dokumenteras eftersom det gör dem tydligare och lättare att kommunicera.

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)