Mälardalens högskola
Box 883
721 23 Västerås

Datum 2011-03-08
Dnr 32-2010-0735

Granskning av intern styrning och kontroll av informationssäkerheten vid Mälardalens högskola 2010

Riksrevisionen har som ett led i den årliga revisionen granskat Mälardalens högskolas (MDH) interna styrning och kontroll av informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa MDH: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 MDH 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 i form av en IT säkerhetspolicy. Det saknas dock fortfarande riktlinjer för att ramverket ska motsvara en etablerad standard. Policyn för IT-säkerhet bör kompletteras med viktiga aspekter rörande informationssäkerhet. De styrdokument som finns behöver uppdateras, och MDH bör formalisera en rutin för regelbundna genomgångar och uppdateringar av dokumenten. Dokumenterade riktlinjer för behörighetsadministration, informationsklassning, kontinuitetsplanering och incidentövervakning

behöver upprättas. Befintlig riskanalys bör kompletteras med mera informationssäkerhet, och MDH behöver åtgärda problemen med nyckelpersonsberoende avseende verksamhetskritiska system. Det finns heller inte någon utsedd person som ansvarar för arbetet med informationssäkerhet vid MDH.

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)
- Myndighetsförordning (2007:515)
- Förordning (2007:603) om intern styrning och kontroll (FISK)
- 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.

FISK definierar arbetet med intern styrning och kontroll som den process som syftar till att myndigheten med rimlig säkerhet fullgör de krav som framgår av 3 § i myndighetsförordningen. FISK föreskriver att myndigheten ska upprätta riskanalyser och vidta kontrollåtgärder samt regelbundet följa upp och dokumentera arbetet.

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. Vid MDH har ansvaret för högskolans säkerhet delegerats till säkerhetsansvarig. Eftersom den som tidigare var säkerhetsansvarig inte längre arbetar vid högskolan har ansvaret för tillfället delegerats om till fastighetsansvarig. Ansvaret omfattar högskolans säkerhet i helhet och består således av ansvar för säkerhet inom ett antal områden. Det är dock ingen som har ett utpekat ansvar specifikt 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* MDH 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 uppdateras

Enligt MSB:s föreskrifter ska myndigheten upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet. MDH hade vid granskningen en upprättad policy för IT-säkerhet. Policyn hade dock inte uppdaterats sedan 2004. Liknande iakttagelser gjordes avseende styrdokument för behörighetsadministration och telefoni.

Eftersom myndigheten saknar uppdaterad dokumenterad styrning för flera viktiga områden medför detta en otydlighet som ökar risken för oönskad hantering av informationstillgångar med möjlig skada för MDH som följd. Riksrevisionen *rekommenderar* MDH att uppdatera sina styrdokument som reglerar hur information ska hanteras vid högskolan. Högskolan bör även formalisera en rutin för regelbundna genomgångar av styrdokument. På detta sätt kan MDH förhindra att dokumenten tappar sin relevans eller blir inaktuella. Policyn för IT-säkerhet bör kompletteras med viktiga aspekter rörande informationssäkerhet. Det kan vara effektivt att bygga dokumentstrukturen kring informationssäkerhetspolicyn och låta denna fungera som ett övergripande dokument. Till policyn är det sedan lämpligt

att koppla underordnade dokument som exempelvis riktlinjer för lösenord och behörighetsadministration.

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. På MDH finns olika rutiner för tilldelning av behörigheter beroende på om det är system där driften sköts av IT-avdelningen, ute på någon avdelning eller av externa leverantörer. Rutinerna 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. Risken med att ha olika rutiner för olika system utan att tillämpa någon gemensam styrning är att riktlinjer kan bli otydliga och svåra att kommunicera.

Riksrevisionen *rekommenderar* MDH 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 behöver kompletteras med informationssäkerhet

MSB anger i sina föreskrifter att myndigheten utifrån en risk- och sårbarhetsanalys ska avgöra hur risker ska hanteras och besluta om åtgärder för myndighetens informationssäkerhet. I enlighet med 3 § FISK har MDH även krav på sig att upprätta riskanalyser för att identifiera omständigheter som utgör risk för att de krav som ställs i 3 § myndighetsförordningen inte fullgörs. Högskolan har inte upprättat några separata riskanalyser avseende informationssäkerhet. Risker förknippade med informationssäkerhet har i begränsad omfattning tagits med i den övergripande riskanalys som högskolan kontinuerligt uppdaterar i enlighet med FISK. MDH har vid flera tillfällen anlitat konsulter för att utvärdera sin IT-verksamhet. I samband med detta har riskanalyser genomförts som delvis rör informationssäkerheten vid högskolan. Ett antal brister har då belysts. Högskolan har gjort insatser avseende en del av bristerna, men flera av dem kvarstår trots att det var förhållandevis länge sedan bristerna rapporterades. Det finns inte heller någon konkret åtgärdsplan för hur de ska komma till rätta med bristerna.

Eftersom högskolan inte genomfört några fullständiga riskanalyser som avser informationssäkerheten kan det försvåra för högskolan att identifiera och avgöra vilka risker som föreligger. Det blir också svårare att bedöma sannolikheten för att det som bedöms riskfyllt inträffar, vilka konsekvenser en riskfyll

händelse kan få för verksamheten samt om risken bör tas med i riskanalysen i enlighet med FISK. En låg medvetenhet om risker och deras konsekvenser kan i sin tur göra det svårt att avgöra vilka åtgärder som ska prioriteras. Risk föreligger dock för att högskolan inte lyckas komma till rätta med bristerna eftersom högskolan inte har någon åtgärdsplan för hur detta ska ske. Resultatet av detta kan bli att högskolan lagt resurser på att analysera risker som inte åtgärdas. Vidare kan fördröjningar av åtgärder innebära att de brister som noterats i arbetet kan ha förändrats vid tidpunkten då de åtgärdas. Detta eftersom analyserna måste möta kontinuerliga och snabba förändringar i informationsmiljön. Eftersom extern hjälp anlitas finns även en risk för att högskolan inte själva tar ställning till de risker och brister som lyfts upp.

Riksrevisionen *rekommenderar* MDH att upprätta en riskanalys som specifikt behandlar högskolans informationssäkerhet. För att den ska utgöra ett bra underlag för prioriteringar bör den även 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. Riskanalyserna bör uppdateras regelbundet för att hållas aktuella. Eftersom miljön för de system som hanterar information förändras snabbt rekommenderar Riksrevisionen att uppdateringar sker vid förändringar. Utifrån riskanalyserna bör högskolan sedan upprätta en handlingsplan med åtgärder och tidpunkter för när åtgärderna ska vidtas.

Eftersom MDH ska upprätta riskanalyser i enlighet med FISK rekommenderar Riksrevisionen att riskerna iakttas och vid behov lyfts upp i högskolans övergripande analys. I de fall högskolan tar in extern hjälp föreslår Riksrevisionen att MDH värderar resultaten och använder dem som underlag för egna riskbedömningar medan de fortfarande är aktuella.

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

MDH 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 riktlinjer för när ledningen på olika nivåer ska informeras, en så kallad eskaleringsprocess. Eftersom incidenter inte loggas, har högskolan mindre möjligheter att upptäcka återkommande problem och lära sig av dessa.

Riksrevisionen *rekommenderar* MDH att upprätta rutiner för övervakning, loggning och hantering av incidenter. Rutinerna bör omfatta samtliga typer av incidenter som kan tänkas uppstå och som 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 MDH förhindra att de återkommer eller föranleder

ytterligare skada. Samtliga rutiner bör dokumenteras eftersom det gör dem tydligare och lättare att kommunicera.

3.6 Rutin för att klassificera information saknas

MSB:s föreskrifter anger att myndigheten ska klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet. MDH bedömer i viss mån den information som finns hos myndigheten. Det finns till exempel en medvetenhet kring hur personuppgifter och sekretessbelagd information ska hanteras. MDH har ingen upprättad rutin för hur högskolan generellt ska klassificera information och i många fall genomförs ingen bedömning förrän informationen efterfrågas.

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* MDH att upprätta riktlinjer för hur högskolan 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.

3.7 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. MDH har inte upprättat någon kontinuitetsplanering för högskolan. 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* MDH 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 Nyckelpersonsberoende

Styrelsen vid MDH har i enlighet med 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 säkrad. MDH har i dag verksamhetskritiska system där endast en person inom MDH har kompetens att utveckla systemen. MDH har startat ett projekt för att minska de risker högskolan förknippar med situationen.

Eftersom endast en person har kompetens att hantera verksamhetskritiska system uppstår 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 systemen.

Riksrevisionen *rekommenderar* MDH fortsätta arbetet med att komma till rätta med nyckelpersonsberoendet. Detta genom att exempelvis sprida utvecklarkompetens på flera personer.

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)