Högskolan i Gävle
801 76 Gävle

Datum 2011-03-08
Dnr 32-2010-0729

Granskning av intern styrning och kontroll av informationssäkerheten vid Högskolan i Gävle 2010

Riksrevisionen har som ett led i den årliga revisionen granskat Högskolan i Gävles (HIG) interna styrning och kontroll av informationssäkerhet.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa HIG: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 HIG 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. HIG:s informationssäkerhetspolicy behöver kompletteras så att den inkluderar även information i ej elektronisk form. HIG har upprättat en systemförvaltningsmodell men har ännu inte fattat beslut avseende modellen. Dokumenterade riktlinjer för riskhantering, informationsklassning och kontinuitetsplaner behöver upprättas. De rutiner som finns avseende behörighetsadministration och incidentövervakning behöver kompletteras samt dokumenteras. HIG behöver upprätta

en rutin för regelbunden uppföljning av arbetet med informationssäkerhet. HIG behöver även överväga ett förstärkt skydd vid uppkoppling för distansarbete.

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 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. HIG 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* HIG 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.

3.2 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. HIG 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 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.

Riksrevisionen *rekommenderar* HIG att upprätta rutiner för regelbunden uppföljning av arbetet med informationssäkerhet. Rutinerna bör säkerställa att ledningen vid högskolan hålls uppdaterade om vilka risker som föreligger och vilka åtgärder som vidtas.

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. HIG 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* HIG 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 Besluta om förvaltningsmodell för samtliga system

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 HIG har upprättat en modell för systemförvaltningen men inte beslutat om den. Formaliserade och dokumenterade förvaltningsmodeller för system 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* HIG att besluta om förvaltningsmodell för sina system.

3.5 Komplettera befintlig informationssäkerhetspolicy med säkerhet för ej elektronisk information

MSB:s föreskrift anger att myndigheten ska upprätta en informationssäkerhetspolicy. HIG har upprättat en policy som avser elektronisk informationssäkerhet. Högskolan har mycket information i ej elektronisk form, men detta inkluderas inte i policyn.

Eftersom informationssäkerhetspolicyn endast omfattar elektronisk information finns risk för att övrig information inte behandlas ur ett informationssäkerhetsperspektiv. Om rutiner och policyer inte omfattar information som inte hålls elektroniskt är det sannolikt att sådan information inte skyddas enligt den standard som satts upp av högskolan. Detta oavsett att den i många fall borde ha samma skyddsvärde som elektronisk information.

Riksrevisionen *rekommenderar* HIG att komplettera sin nuvarande informationssäkerhetspolicy så att den inkluderar all information vid myndigheten.

3.6 Riktlinjer för klassning av information saknas

MSB:s föreskrifter anger att myndigheten ska klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet. HIG skyddar i dag viss information extra, till exempel information om personal vid högskolan samt känsliga forskningsresultat. HIG genomför dock ingen klassning av information.

Risken med att inte göra någon klassning av informationen 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 informationen 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* HIG att upprätta riktlinjer för hur de 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 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. HIG har informella rutiner för hantering av incidenter. Rutinerna är inte formaliserade eller dokumenterade och det finns ingen samlad rutin för rapportering av incidenter.

HIG 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.

Riksrevisionen *rekommenderar* HIG att upprätta rutiner för övervakning 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 HIG förhindra att de återkommer eller leder till ytterligare skada. Samtliga rutiner bör dokumenteras eftersom det gör dem tydligare och lättare att kommunicera.

3.8 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. HIG har inte upprättat någon kontinuitetsplanering för högskolan. En återstartsplan finns men den anges vara inaktuell.

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 uppdaterad 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* HIG att upprätta och dokumentera en kontinuitetsplanering. Denna bör innefatta en uppdaterad återstartsplan där verksamhetskritiska system prioriteras. På detta sätt kan högskolan öka möjligheten att hantera eventuella nedgångar i systemen på ett effektivt sätt.

3.9 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 HIG:s 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 att ha en sådan 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 förenklar intrång i HIG:s system med förvanskning, förstörelse och stöld av information som en möjlig följd.

Riksrevisionen *rekommenderar* HIG 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 HIG risken för otillbörliga intrång i nätverket.

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)