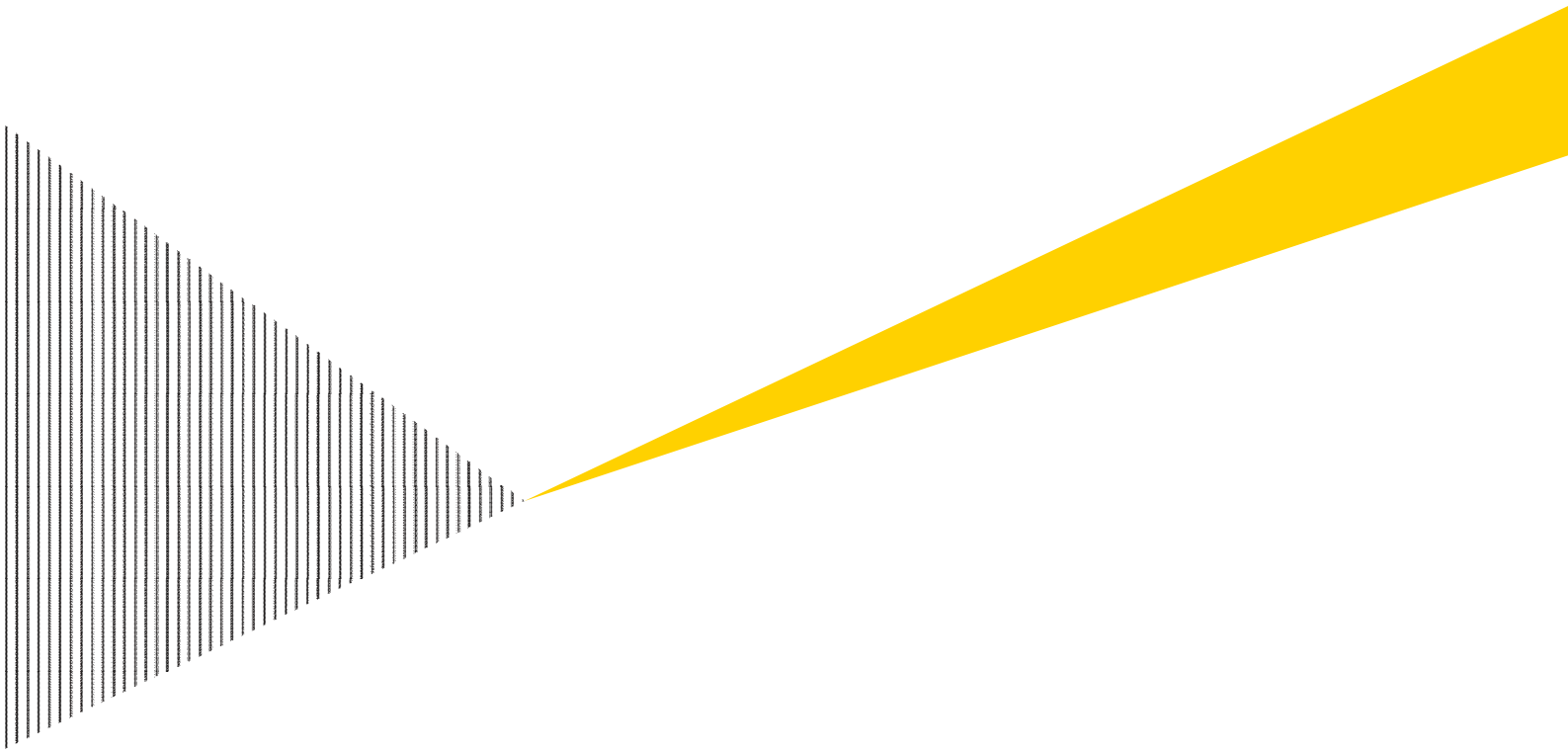
Revisionsrapport 3/2010
Genomförd på uppdrag av revisorerna
maj/sept 2010



Haninge kommun

Rapport: IT-revision, granskning av informationssäkerheten

ERNST & YOUNG

Sammanfattning

Bakgrund

På uppdrag av de förtroendevalda revisorerna i Haninge kommun har Ernst & Young genomfört en IT-revision i kommunen. IT-revisionens syfte har varit att granska och bedöma informationssäkerheten på en övergripande nivå i kommunen. Granskningen har gjorts mot Myndigheten för samhällsskydd och beredskaps ramverk för informationssäkerhet, BITS.

Övergripande slutsatser

Av samtliga granskningspunkter är fördelningen av bedömningarna följande:

Kontrollen finns ej eller fungerar ej tillfredsställande:	**24 %**
Kontrollen finns och fungerar delvis:	**25 %**
Kontrollen finns och fungerar tillfredsställande:	**49 %**
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	**2 %**

Jämfört med andra kommuner som Ernst & Young gjort liknande granskningar för ligger Haninge kommuns måluppfyllnad ungefär på kommungenomsnittet.

Iakttagelser

Fullständiga iakttagelser med riskbedömningar och rekommendationer finns i kapitel 4.

#	Iakttagelse	Prioritet
1.	Bristande behörighetsrutiner	Hög
2.	Kontinuitetsplaner saknas	Hög
3.	Omfattande tillgång till datorhallen	Hög
4.	Avsaknad av formell rutin för beslut om programförändringar	Hög
5.	Inaktuell informationssäkerhetspolicy	Medel
6.	Ej fullständig driftsdokumentation	Medel
7.	Formella regler saknas för informationsklassning	Medel
8.	Avsaknad av IT-strategi	Låg

Innehållsförteckning

1 Bakgrund

1.1 Syfte

Idag bedrivs så gott som all verksamhet i en kommun med någon form av datoriserat stöd. Stödet har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet. För att uppnå målen för kommunens verksamheter krävs att informationen i verksamhetsstödet är tillgängligt, riktigt och har korrekt konfidentialitet samt är spårbart.

På uppdrag av de förtroendevalda revisorerna i Haninge kommun har Ernst & Young genomfört en IT-revision i kommunen. IT-revisionens syfte har varit att granska och bedöma informationssäkerheten på en övergripande nivå i kommunen.

Syftet har också varit att jämföra kommunens nuvarande informationssäkerhet mot BITS, Myndigheten för samhällsskydd och beredskaps (tidigare Krisberedskapsmyndigheten) ramverk för informationssäkerhet. BITS står för *Basnivå för informationssäkerhet* och har sitt ursprung i den internationella informationssäkerhetsstandarden ISO/IEC 27000.

1.2 Metod

Baserat på erfarenheter från tidigare kommunrevisioner har Ernst & Young valt ut ett antal relevanta kontroller som presenteras i BITS, fördelat på elva huvudområden:

1. Säkerhetspolicy
2. Organisation av säkerheten
3. Hantering av tillgångar
4. Personalresurser och säkerhet
5. Fysisk och miljörelaterad säkerhet
6. Styrning och kommunikation av drift
7. Styrning av åtkomst
8. Anskaffning, utveckling och underhåll av informationssystem
9. Hantering av informationssäkerhetsincidenter
10. Kontinuitetsplanering i verksamheten
11. Efterlevnad

Rapporten redovisar i vilken grad kommunen uppfyller valda rekommendationer ur BITS. Resultatet är en sammanvägd bedömning, som baseras på information som lämnats vid intervjuerna samt genom erhållen dokumentation. Den sammanvägda bedömningen av svaren på kontrollerna har bedömts enligt följande alternativ:

Nej	Kontrollen finns ej eller fungerar ej tillfredsställande.
Delvis	Kontrollen finns och fungerar delvis.
Ja	Kontrollen finns och fungerar tillfredsställande.
E/T	Ej tillämplig, kontrollen behövs ej av särskilda skäl.

Analysen baseras på erhållen dokumentation samt på intervju med Johan Högne (konsult, operativ IT-chef), Rolf Wessung (teknisk systemförvaltare) och Per Ståhl (konsult, delaktig i pågående IT-driftupphandling). Ytterligare information har inhämtats från Inger Karlberg (systemförvaltare för verksamhetssystemen Procapita och WM Omsorg). Ansvaret för informationssäkerhet delas mellan kommunens säkerhetsansvarige och IT-strategen.

Arbetet har genomförts av Marcus Hansson och Anna Wibring under maj 2010 och kvalitetssäkrats av Pelle Söderberg.

De intervjuade har fått möjlighet att faktagranska rapporten.

1.3 Avgränsningar

Iakttagelser och analyser baseras enbart på information som har inhämtats vid intervjuer och förelagd dokumentation. Inga tester har genomförts. Det kan finnas brister i kommunens hantering av IT som vi inte har identifierat. Arbetet har inte omfattat test av generella IT-kontroller och applikationskontroller.

2 Iakttagelser

2.1 IT-organisation

Kommunens IT-avdelning har 15 anställda, samt ytterligare 5-7 konsulter i verksamheten.

Bland rollerna i IT-organisationen finns IT-chef (1), teknisk systemförvaltare (1), IT-koordinatorer (2), nätansvarig (1), service desk (3), PC-support (2), systemtekniker (5) och inköpsansvarig (1). Flera roller i kommunens IT-organisation innehas av inhyrda konsulter, bland annat rollen som IT-chef.

Beställarsidan representeras av kommunens IT-strateg.

2.2 IT-system

Kommunen har ca 77 000 invånare och 70 olika verksamhetssystem. Ett urval av de för verksamheten mest betydande systemen och deras huvudsakliga funktion listas i tabellen nedan. Kommunen har ansvar både för skolsystemet och för administrativa systemet.

Haninge kommun har totalt ca 3 300 anställda och 11 000 elever med egna konton.

System	Beskrivning	Leverantör
Agresso	Ekonomisystem	Agresso
CMG (NICE)	Hänvisningssystem	TeliaSonera
Dexter/Extens	Skolsystem	IST
EPiServer	Kommunhemsida	EPiServer
GroupWise	e-postsystem	Novell
Heroma	PA-system	Logica
KommunOffice	Diaresystem	Triplan
MMK	Ärendehanteringssystem	Vendel Data
Procapita	Omsorgssystem	TietoEnator
Solen WEB	GIS-system	Cartesia
Time Care	Tidplaneringssystem	Time Care
WM Omsorg	Omsorgssystem	Logica

2.2.1 Aktuella förändringar

Tillsammans med Södertälje och Nynäshamn kommuner pågår just nu en upphandling av all IT-drift. Visionen är att all drift ska vara outsourcad framöver, och att allt ska vara genomfört innan den 1 januari 2011. I samband med detta kommer stora delar av IT-funktionen och relaterade dokument att förändras, inklusive rutiner och riktlinjer. Den nu genomförda IT-revisionen ger dock en ögonblicksbild av verksamheten i maj 2010.

2.3 Granskningsprotokoll

Granskningspunkt		Kommentar	Utvärdering
1 Säkerhetspolicy			
1.1	Har kommunen en informations-/IT-säkerhetspolicy?	Kommunen har en informationssäkerhetspolicy från 2001. Policyn berör på en mycket övergripande nivå hur kommunen ska upprätthålla en säker informationshantering.	Delvis
2 Organisation av säkerheten			
2.1	Finns det en informationssäkerhetssamordnare/-funktion för informationssäkerhet?	Ansvaret delas mellan säkerhetsansvarig och IT-strateg. Uppdelningen är ej formaliserad.	Delvis
2.2	Har ledningen utsett systemägare för samtliga informationssystem?	Ja.	Ja
2.3	Har organisationen utsett systemansvariga?	Ja, systemförvaltare.	Ja
2.4	Finns det en samordningsfunktion för att länka samman den operativa verksamheten för informationssäkerhet och ledningen?	Ja, en IT-styrgrupp i vilken koncernledning, IT-chef, IT-strateg och serviceenhetens chef ingår.	Ja
2.5	Har ansvaret för informationssäkerheten reglerats i avtal för informationsbehandling som lagts ut på en utomstående organisation?	Nej, detta är ej reglerat i avtal i dagsläget.	Nej
3 Hantering av tillgångar			
3.1	Är organisationens information klassad avseende sekretess/riktighet/tillgänglighet?	Nej.	Nej
3.2	Har samtliga informationssystem identifierats och dokumenterats i en aktuell systemförteckning?	Ja, senast uppdaterad hösten 2009.	Ja
3.3	Finns det en ansvarsfördelning för organisationens samtliga informationstillgångar?	Ja, förvaltningschef för respektive förvaltning ansvarar för informationen i systemen.	Ja
3.4	Finns det upprättat dokument för hur informationsbehandlings-resurser får användas?	Nej.	Nej
4 Personalresurser och säkerhet			
4.1	Får inhyrd/inlånad personal information om vilka säkerhetskrav och instruktioner som gäller?	För detta hänvisas inhyrd/inlånad personal till intranätet. I kvittensen alla enskilda användare gör av ett nytt nätverkskonto förbinder man sig att följa kommunens policy för e-post, internet och informationssäkerhet. Detta gäller även inhyrd/inlånad personal.	Delvis
4.2	Har systemägaren definierat vilka krav som ställs på användare som får tillgång till informationssystem och information?	Nej, som regel inte.	Nej
4.3	Finns det framtagna dokumenterade säkerhetsinstruktioner för användare?	Ja, dels i *IT-handbok med användaren i centrum* (senast uppdaterad i juli 2003) och dels i *IT-säkerhetsinstruktion för användare* (senast uppdaterad i september 2004).	Ja
4.4	Genomförs utbildningsinsatser inom informationssäkerhet regelbundet?	Nej.	Nej
4.5	Finns det användarhandledning för ett informationssystem att tillgå?	Styrs ej centralt, utan ansvaret vilar på respektive systemägare. För många system finns användarhandledningar att tillgå.	Delvis
4.6	Dras åtkomsträtten till information och informationsbehandlingsresurser in vid avslutande av anställning eller vid förflyttning?	Aktuell förvaltning/avdelning ska skicka en blankett till IT-avdelningen som inaktiverar användaren i Active Directory. Att ta bort användaren ur verksamhetssystemet är upp till respektive förvaltning.	Delvis

Granskningspunkt		Kommentar	Utvärdering
5 Fysisk och miljörelaterad säkerhet			
5.1	Finns funktioner för att förhindra obehörig fysisk tillträde till organisationens lokaler och information?	Ja.	Ja
5.2	Har IT-utrustning som kräver avbrottsfri kraft identifierats?	Ja.	Ja
5.3	Finns larm kopplat till larmmottagare för: - brand, temperatur, fukt? - sker test till larmmottagare?	Ja. Testning utförs av leverantören en gång per år.	Ja
5.4	Finns i direkt anslutning till viktig datorkommunikationsutrustning kolsyresläckare?	Ja, i datorhallen.	Ja
5.5	Regleras tillträde till utrymmen med känslig information eller informationssystem utifrån informationens skyddsbehov? Tillträdesrättigheter, rutiner för upprättande?	Inga särskilda rutiner finns. För att få behörighet att gå in i datorhallen krävs att tillträde godkänns muntligt av husets intendenturchef. Det finns ingen rutin för att se över tillträdesrättigheter med jämna mellanrum. Ett 60-tal personer har tillgång till datorhallen.	Nej
5.6	Är korskopplingsskåp låsta?	Ja.	Ja
5.7	Raderas känslig information på ett säkert sätt från utrustning som tas ur bruk eller återanvänds?	Hårddiskar från datorer som tas ur bruk ska skickas på destruktion.	Ja
5.8	Finns särskilda säkerhetsåtgärder för utrustning utanför ordinarie arbetsplats?	Ja, för användaren finns *Riktlinjer för distansarbete i hemmet* (senast uppdaterad 2005). Den tekniska lösningen är en VPN-uppkoppling. Tvåfaktorsautenticering används.	Ja
5.9	Finns information och regler som förklarar att informationsbehandlingsresurser inte får föras ut från organisationens lokaler utan medgivande från ansvarig chef?	Nej.	Nej
6 Styrning och kommunikation av drift			
6.1	Finns det driftdokumentation för verksamhetskritiska informationssystem?	Delvis, dock inte alltid detaljerad.	Delvis
6.2	Är klockorna i informationssystemen synkroniserade med godkänd exakt tidsangivelse?	Ja.	Ja
6.3	Sker system-/programutveckling samt tester av modifierade system åtskilt från driftmiljön?	Ingen systemutveckling görs i kommunen. För vissa system utförs acceptanstestning i testmiljö.	Delvis
6.4	Finns rutiner för hur utomstående leverantörers tjänster följs upp och granskas?	Nej, inga rutiner för detta.	Nej
6.5	Godkänner lämplig personal (systemägaren) driftsättningar av förändrade informationssystem?	Ja, som regel gör systemförvaltaren eller motsvarande detta. Det är dock upp till de enskilda förvaltningarna.	Ja
6.6	Finns det för både servrar och klienter rutiner för skydd mot skadlig programkod?	Ja, uppdatering av skyddet sker automatiskt.	Ja
6.7	Har organisations nätverk delats upp i mindre enheter (segmentering), så att en (virus) attack enbart drabbar en del av nätverket?	Ja, nätverket är uppdelat bland annat i skolnät, administrativt nät, resursnät samt publika gästnät.	Ja
6.8	Genomförs säkerhetskopiering regelbundet?	Ja, inkrementell säkerhetskopiering görs varje natt. Full säkerhetskopiering görs en gång per vecka. Banden förvaras skilda från servrarna i samma byggnad men i en annan brandcell.	Ja

Granskningspunkt		Kommentar	Utvärdering
6.9	Genomförs regelbundna tester för att säkerställa att informationssystem kan återstartas från säkerhetskopior?	Enbart stickprovstester.	Delvis
6.10	Finns det en aktuell förteckning över samtliga externa anslutningar?	Ja.	Ja
6.11	Saknas alternativa vägar vid sidan av organisationens brandvägg in till det interna nätverket?	Ja.	Ja
6.12	Är det möjligt att logga säkerhetsrelevanta händelser?	Ja, för brandväggen.	Delvis
6.13	Finns det riktlinjer avseende förvaringstid för datamedia?	Nej.	Nej
6.14	Finns det dokumenterade regler avseende vilken information som får skickas utanför organisationen?	Nej, dokumenterad policy finns ej. Hantering av viss information styrs av sekretesslagstiftningen.	Nej
6.15	Gäller det för e-postsystem och andra viktiga system att de är isolerade från externa nät? (DMZ) t.ex. genom någon form av brandväggsfunktion?	Ja.	Ja
6.16	Sparas revisionsloggar för säkerhetsrelevanta händelser?	Loggar för brandväggen sparas i tre månader.	Delvis
7 Styrning av åtkomst			
7.1	Har organisationen satt upp dokumenterade regler för åtkomst/tillträde för tredjeparts åtkomst till information eller informationssystem?	Nej, inga dokumenterade regler finns. Det finns inte heller några rutiner för att sätta ett slutdatum för konsulters åtkomst till system.	Nej
7.2	Tilldelas användare en behörighetsprofil som endast medger åtkomst till informationssystem som krävs för att lösa arbetsuppgifterna?	Användare tilldelas behörigheter enligt en beställningsblankett som aktuell chef fyller i.	Ja
7.3	Begränsas rätten att installera nya program i nätverket samt den egna arbetsstationen till endast utsedd behörig personal?	Användarna har hittills inte varit lokala administratörer på sina datorer, vilket de dock är från och med nu.	Delvis
7.4	Har samtliga administratörer fullständiga systembehörigheter, eller endast i den utsträckning som krävs för arbetsuppgifterna?	Administratörer har som regel behörighet i den utsträckning som behövs för arbetet. Det finns inga formaliserade rutiner, utan IT-chefen beslutar och meddelar muntligt.	Delvis
7.5	Har organisationen en dokumenterad rutin för tilldelning, borttag eller förändring av behörighet? Är de kommunicerade till ansvarig för behörigheter?	För tilldelning av behörighet till kommunens administrativa nätverk ska avsedd blankett användas, vilken ska signeras av närmast ansvarig chef.	Delvis
7.6	Får nya användare ett initialt lösenord som de måste byta, till ett eget valt lösenord vid första användning?	Ja, när det gäller lösenord som administreras av IT-avdelningen.	Ja
7.7	Genomförs kontinuerlig (minst en gång per år) kontroll av organisationens behörigheter?	Nej, inte centralt. Rutinerna för olika verksamhetssystem skiljer sig åt mellan förvaltningarna.	Nej
7.8	Har systemadministratörer/-tekniker/-användare individuella unika användaridentiteter?	Ja.	Ja
7.9	Öppnas låsta användarkonton först efter säker identifiering av användaren?	Ja, låsta användarkonton öppnas efter motringning.	Ja
7.10	Finns en gemensam lösenords-policy?	Nej, inte som gäller för alla system. För det administrativa nätet krävs ett lösenord med åtta tecken som ska bytas var 6:e månad.	Delvis

Granskningspunkt		Kommentar	Utvärdering
7.11	Sker automatisk aktivering av skärmsläckare och automatisk låsning av obevakade arbets-stationer efter visst givet tidsintervall? Upplåsning kan endast ske med lösenord.	Ja.	Ja
7.12	Är brandväggsfunktionen den enda kanalen för IP-baserad datakommunikation till och från organisationen?	Ja.	Ja
7.13	Finns en dokumenterad brandväggspolicy där det beskrivs vilka tjänster brandväggen skall tillhandahålla?	Nej.	Nej
7.14	Används trådlösa lokala nät? I så fall, finns det åtgärder mot obehörig avlyssning och obehörigt utnyttjande av resurser?	Ja, det finns både publikt och internt trådlöst nätverk. Det interna är krypterat.	Ja
7.15	Finns det en karta över nuvarande säkerhetsarkitektur (tekniska anvisningar) för interna och externa nät och kommunikationssystem?	Ja.	Ja
7.16	Har organisationen upprättat dokumenterade riktlinjer avseende lagring?	Ja. Detta beskrivs i *IT-säkerhetsinstruktion för användare* (2004).	Ja
7.17	Har verksamheten ställt och dokumenterat tekniska säkerhetskrav och krav på praktisk hantering avseende användandet av mobil datorutrustning och distansarbete?	Ja. VPN-uppkoppling används vid distansarbete. Krav för distansarbete finns dokumenterade i *Riktlinjer för distansarbete i hemmet* (2005).	Ja
7.18	Har systemägaren eller motsvarande beslutat om att ett informationssystems information ska få bearbetas på distans med stationär eller mobil utrustning?	Ja, i vissa fall. Detta är systemägarens ansvar.	Delvis
7.19	Finns det aktuell dokumentation med regler för distansarbete?	Regler för distansarbete finns dokumenterade i *Riktlinjer för distansarbete i hemmet* (2005).	Ja
8 Anskaffning, utveckling och underhåll av informationssystem			
8.1	Har en systemsäkerhetsanalys upprättats och dokumenterats för varje informationssystem som bedöms som viktigt?	Ja, för ett 40-tal servrar.	Ja
8.2	Krypteras persondata som förmedlas över öppna nät?	Ja.	Ja
8.3	Finns det angiven personal som ansvarar för systemunderhåll?	Ja.	Ja
8.4	Finns det regler för hur system- och programutveckling ska genomföras?	Kommunen har ingen egen systemutveckling.	Ej tillämpligt
8.5	Finns det regler och riktlinjer avseende beslut om programändringar?	Nej.	Nej
8.6	Finns det dokumenterade rutiner för hur utbildning ska genomföras för köpta system? Omfattar rutinen även kompletterande utbildning vid program- och funktionsändringar?	Detta är upp till varje verksamhetsområde. Utbildningsinsatser genomförs som regel för de större systemen.	Delvis
8.7	Finns det en uppdaterad och aktuell systemdokumentation för informationssystemen?	Man har inga egenutvecklade system.	Ej tillämpligt

Granskningspunkt		Kommentar	Utvärdering
9 Hantering av informationssäkerhetsincidenter			
9.1	Finns det dokumenterade instruktioner avseende vart användare skall vända sig och hur de skall agera vid funktionsfel, misstanke om intrång eller vid andra störningar?	Ja, i *IT-handbok med användaren i centrum* (2003).	Ja
10 Kontinuitetsplanering i verksamheten			
10.1	Finns det en gemensam kontinuitetsplan dokumenterad för organisationen?	Nej.	Nej
10.2	Har systemägaren eller motsvarande beslutat om den längsta acceptabla tid som informationssystemet bedöms kunna vara ur funktion innan verksamheten äventyras?	Nej.	Nej
10.3	Finns det en dokumenterad avbrottsplan med återstarts- och reservrutiner för datadriften som vidtas inom ramen för ordinarie driften?	Delvis. För datorhallen finns en driftpärm som beskriver rutinerna. För olika verksamhetssystem skiljer det sig åt mellan förvaltningarna.	Delvis
10.4	Har omständigheter som ska betecknas som kris/katastrof (extraordinära händelser) för verksamheten kartlagts?	Nej.	Nej
11 Efterlevnad			
11.1	Användas endast programvaror i enlighet med gällande avtal och licensregler?	Inventering pågår.	Delvis
11.2	Har organisationen förtecknat och anmält personuppgifter till personuppgiftsombud?	Ja, detta är kommunjuristens område.	Ja
11.3	Genomförs interna och externa penetrationstester kontinuerligt?	Det finns inga rutiner för kontinuerliga penetrationstester. Det har dock genomförts två gånger.	Delvis
11.4	Granskar ledningspersoner regelbundet att säkerhetsrutiner, -policy och -normer efterlevs?	Nej, inte regelbundet. Rutinerna varierar.	Nej

3 Jämförelse mot andra kommuner

Ernst & Young har gjort ett flertal gapanalyser mot BITS hos Sveriges kommuner. Tack vare detta kan vi mäta Haninge kommuns mognadsgrad rörande informationssäkerhet mot ett genomsnitt av de kommuner vi granskat.

I diagrammet nedan representerar ytterkanten 100 % måluppfyllnad, medan mittpunkten anger 0 % måluppfyllnad. Siffrorna anger respektive område i BITS enligt:

1. Säkerhetspolicy
2. Organisation av säkerheten
3. Hantering av tillgångar
4. Personalresurser och säkerhet
5. Fysisk och miljörelaterad säkerhet
6. Styrning och kommunikation av drift
7. Styrning av åtkomst
8. Anskaffning, utveckling och underhåll av informationssystem
9. Hantering av informationssäkerhetsincidenter
10. Kontinuitetsplanering i verksamheten
11. Efterlevnad

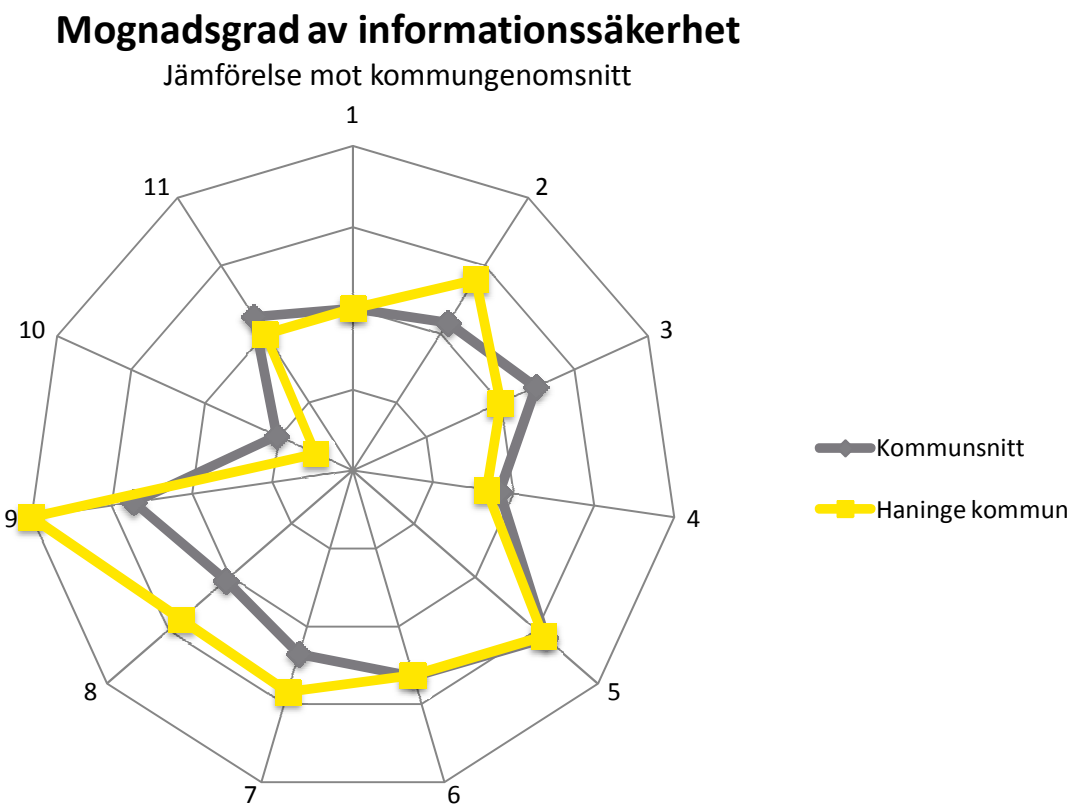


Bild 3.1 Kommun jämförelse mognadsgrad

4 Slutsatser och rekommendationer

4.1 Generella slutsatser

Av samtliga granskningspunkter är fördelningen av bedömningarna följande:

Nej	Kontrollen finns ej eller fungerar ej tillfredsställande:	**24 %**
Delvis	Kontrollen finns och fungerar delvis:	**25 %**
Ja	Kontrollen finns och fungerar tillfredsställande:	**49 %**
E/T	Ej tillämplig, kontrollen behövs ej av särskilda skäl:	**2 %**

Kommunens **starkaste** områden är:

- Organisation av säkerheten
- Fysisk och miljörelaterad säkerhet
- Hantering av informationssäkerhetsincidenter

Kommunens **svagaste** områden är:

- Kontinuitetsplanering i verksamheten
- Hantering av tillgångar
- Personalresurser och säkerhet

4.2 Rekommendationer

Nedan följer våra rekommendationer samt ett förslag på prioritering. Rekommendationerna är prioriterade enligt följande:

Hög	Nyckelkontroll ej på plats/ej effektiv. Bristen bör åtgärdas snarast för att säkerställa god intern kontroll på kort sikt.
Medel	Nyckelkontroll delvis på plats/delvis effektiv. Bristen bör åtgärdas för att säkerställa god intern kontroll på lång sikt.
Låg	Nyckelkontroll på plats men effektivitet kan förbättras. Bristen bör åtgärdas på lång sikt.

#	Iakttagelse och rekommendation	Prioritet
1.	Iakttagelse: Bristande behörighetsrutiner Vi har noterat att det saknas dokumenterade rutiner för förändring och borttag av behörigheter till kommunens nätverk och system. Vi har också noterat att det saknas generella riktlinjer för genomgång av behörigheter till nätverk och verksamhetssystem. För vissa verksamhetssystem kan den enskilda förvaltningen dock ha skapat egna rutiner. Risk: Att inte ha en komplett rutin för behörighetsadministration ökar risken att icke-auktoriserade personer får åtkomst till system och information. Att inte genomföra genomgång av behörigheter i system och nätverk ökar risken för att personer som slutat eller bytt tjänst fortfarande har tillgång till system och information. Rekommendation: Vi rekommenderar Haninge kommun att dokumentera och implementera en enhetlig process för att skapa nya/ta bort/förändra rättigheter i systemen och nätverket, samt att dokumentera och implementera en enhetlig rutin för att granska rättigheter i systemen. Följande kontroller och aktiviteter bör finnas med: • Det skall framgå vem som får beställa nya/borttag/ändrade rättigheter (vanligtvis enhetschef eller personalavdelning) • Mottagare av beställning bör kontrollera att beställaren har befogenheter att göra beställning • Information om att konto har skapats bör skickas med kopia till beställaren • Kontouppgifter bör ej skickas okrypterade över publika nätverk • Användaren bör byta lösenord vid första inloggning • Det bör vara klarlagt vem som ansvarar för att en person som slutar ej längre har rättigheter till systemen (enhetschef eller personalavdelning) • IT-avdelningen bör förse enhetschefer med listor över behörigheter två gånger per år • Enhetschefer bör gå igenom listorna, markera felaktigheter, signera samt sända tillbaka listorna till IT-avdelningen • IT-avdelningen tar bort eller förändrar rättigheter enligt underlag	Hög

#	Iakttagelse och rekommendation	Prioritet
2.	Iakttagelse: Kontinuitetsplaner saknas Vi har ej identifierat några existerande kontinuitetsplaner. Risk: Avsaknad av formell kontinuitetsplanering ökar risken för att avbrott ej hanteras på ett för verksamheten optimalt sätt. Vidare är sannolikheten att verksamheten skall drabbas av incidenter högre om kontinuitetsplaner saknas. Rekommendation: Vi rekommenderar Haninge kommun att skapa rutiner för kontinuitetsplanering. Rutinerna bör utgå från en processbaserad riskanalys och adressera: • Reservrutiner vid avbrott för tänkta scenarios • Rutiner för återställning av system • Rutiner för återskapande av förlorad information • Rutiner för inmatning av data från reservrutiner • Periodisk testning av rutiner	Hög
3.	Iakttagelse: Omfattande tillgång till datorhallen Ett 60-tal personer har tillgång till datorhallen. Tillträdesrätt ges muntligt och ingen periodisk genomgång av behörigheter genomförs. Risk: Att inte ha en robust rutin för behörighetsadministration för datorhallen kan öka risken att icke-auktoriserade personer får åtkomst till servrar. Avsaknad av periodisk genomgång ökar risken för att personer som inte längre är beroende av tillträde till datorhallen i sitt arbete har tillgång till känslig information. Rekommendation: Vi rekommenderar Haninge kommun att säkerställa att behörighet till datorhallen är begränsad och endast ges de anställda och den inhyrda personal som är beroende av tillträde i sitt arbete. Vi rekommenderar också att behörighetsrutiner dokumenteras och att tillträdesmedgivande ges skriftligen, samt att periodisk genomgång görs.	Hög

#	Iakttagelse och rekommendation	Prioritet
4.	Iakttagelse: Avsaknad av formell rutin för beslut om programförändringar Vi har noterat att kommunen saknar regler och riktlinjer som avser beslut om programförändringar. Risk: Att inte ha en dokumenterad och förankrad rutin för beslut om och godkännande av programförändringar ökar risken för att icke godkända förändringar implementeras vilket i sin tur kan leda till att systemet ej stödjer verksamheten på ett optimalt sätt. Rekommendation: Vi rekommenderar Haninge kommun att skapa en rutin för beslut om programförändringar. Följande kontroller och aktiviteter bör finnas med: • Om skillnad skall göras mellan processen för stora och små förändringar bör det tydligt definieras vad en stor och en liten förändring innebär • Det skall framgå vem som får beställa förändringar • Alla beställningar av förändringar skall vara dokumenterade • Beställning skall godkännas av systemägare (eller motsvarande) • Acceptanstest av förändring skall göras i miljö separerad från produktionsmiljö. Testfall i testprotokoll bör vara länkade till krav i beställning • Testresultat skall godkännas av systemägare (eller liknande) Vid större förändringar bör uppföljning av förändringens verksamhetsnytta göras.	Hög
5.	Iakttagelse: Inaktuell informationssäkerhetspolicy Vi har noterat att kommunen har en inaktuell informationssäkerhetspolicy. Den nuvarande är daterad till 2001. Risk: Ej uppdaterad informationssäkerhetspolicy kan leda till ett ökat antal incidenter där känslig information förloras, förvanskas eller exponeras. Rekommendation: Vi rekommenderar kommunen att uppdatera informationssäkerhetspolicy som täcker tillämpbara krav i den internationella informationssäkerhetsstandarden ISO/IEC 27000, alternativt BITS. Dessa krav innefattar riskhantering, organisation, informationsklassning, personalsäkerhet, fysisk säkerhet, kommunikation och drift, styrning av åtkomst, utveckling och förvaltning, incidenthantering, kontinuitetsplanering och efterlevnad. Det bör tydligt framgå att ledningen står bakom informationssäkerhetsarbetet. Vi rekommenderar också kommunen att uppdaterar den/de lathundar för användare som täcker lösenordshantering samt användning av internet, e-post och datorutrustning.	Medel
6.	Iakttagelse: Ej fullständig driftsdokumentation Vi har noterat att driftsdokumentation ej är fullständig. Risk: Avsaknad av och/eller bristande kvalitet i driftdokumentation ökar nyckelpersonberoende, kan minska effektivt användande av system, samt kan försvåra återstart av system i samband med avbrott. Rekommendation: Vi rekommenderar Haninge kommun att kartlägga existerande driftdokumentation samt åtgärda de brister som identifieras.	Medel

#	Iakttagelse och rekommendation	Prioritet
7.	Iakttagelse: Formella regler saknas för informationsklassning Vi har noterat att kommunen saknar regler för informationsklassning. Risk: Att inte ha klara regler kring informationsklassning kan öka risken att konfidentiell och/eller känslig information kommer i orätta händer. Rekommendation: Vi rekommenderar Haninge kommun att upprätta en informationsklassningspolicy som definierar informationsklasser samt anger hur informationen per respektive klass skall hanteras.	Medel
8.	Iakttagelse: Avsaknad av IT-strategi Haninge kommun har ingen IT-strategi kopplad till verksamhetsmål. Risk Avsaknad av IT-strategi kan leda till att IT-verksamheten ej stödjer och utvecklar den ordinarie verksamheten på ett effektivt sätt. Rekommendation Det saknas i dagsläget en uppdaterad strategi på lång sikt vilket kan leda till att fel prioriteringar görs i pågående och planerade projekt och investeringar. Vi rekommenderar att kommunen tar fram en IT-strategi som beskriver hur IT på bästa sätt skall stödja och utveckla verksamheten.	Låg

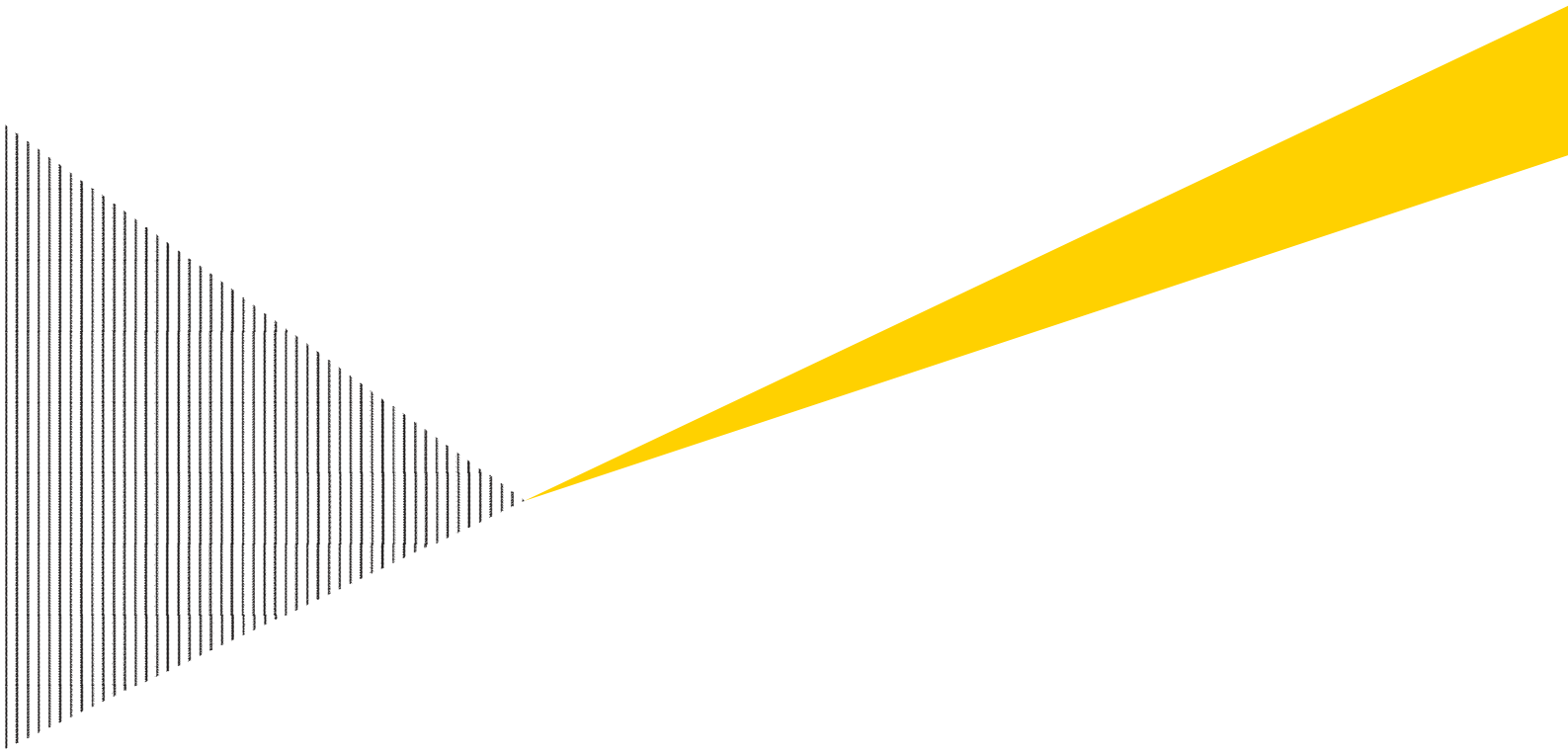
4.3 Övriga rekommendationer

Vi rekommenderar också kommunen att:

- Identifiera de mest verksamhetskritiska systemen och utföra riskanalyser på dessa tillsammans med systemägare, exempelvis i samband med framtagande av kontinuitetsplaner.
- Utbilda personalen i informationssäkerhet.
- Ta fram regler för loggning.
- Ta fram rutiner för hur utomstående leverantörers tjänster ska granskas och följas upp.
- Ta fram regler för lagring och arkivering av information.
- Kontrollera efterlevnad av framtagna policys och riktlinjer.
- Ta fram en lösenordspolicy som gäller för kommunen samtliga verksamhetssystem.
- Ta fram en brandväggspolicy.

Ovanstående rekommendationer är ej prioriterade.

Göteborg den 8 september 2010



Marcus Hansson
marcus.hansson@se.ey.com
031-63 63 26

Anna Wibring
anna.wibring@se.ey.com
031-63 63 20