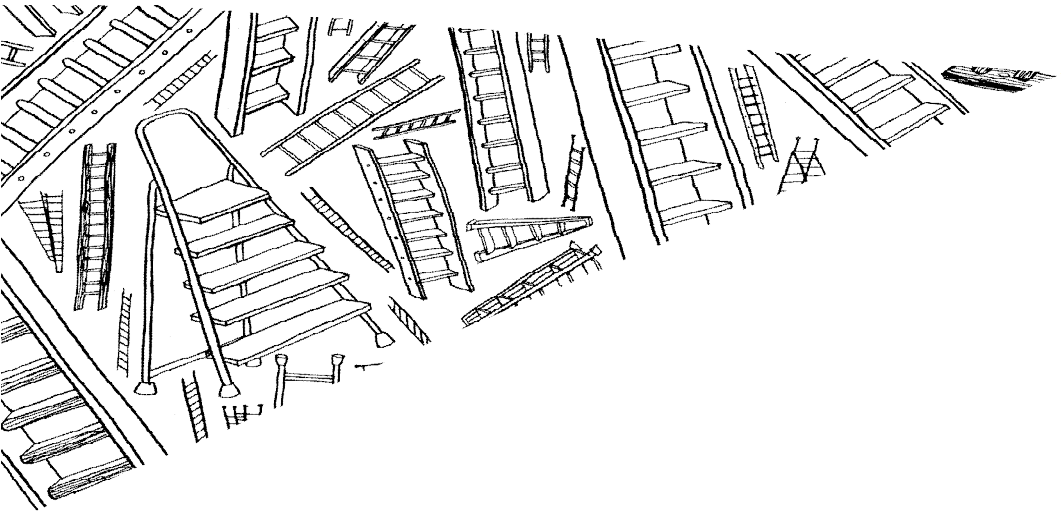
Revisionsrapport 2014
Genomförd på uppdrag av revisorerna

Granskning rörande kommunens hantering av IT

Haninge kommun



Innehåll

1. Sammanfattning 3

2. Inledning 4

2.1. Bakgrund 4
2.2. Syfte och revisionsfrågor 4
2.3. Ansvarig nämnd 5
2.4. Granskningens genomförande 5

3. Kommunens organisation med avseende på IT 5

3.1. Övergripande struktur avseende drift av IT inom kommunen 5
3.2. Pågående förändringsarbete med avseende på hantering av IT 5

4. Bedömning utifrån revisionsfrågorna 6

4.1. Hur säkerställs informationssäkerhet samt funktionalitet och säkerhet i de väsentliga IT-system som kommunen använder? 6
4.2. Är ansvarsfördelningen för kommunens IT-hantering tydlig? 6
4.3. Finns tydliga styrdokument (policy, riktlinjer etc.) och följs efterlevnaden av dessa upp regelbundet? 7
4.4. Genomförs regelbundna riskanalyser av IT-systemen? I så fall, hur ofta? 8
4.5. Görs uppföljningar av IT-kostnader? 8
4.6. Hur arbetar kommunen med IT-konsulter, i synnerhet upphandling, styrning och uppföljning av IT-tjänster? 8

5. Slutsatser och rekommendationer 9

1. Sammanfattning

År 2010 genomfördes en betydande förändring av Haninge kommuns IT-arbete då drift av IT-system lades ut på extern leverantör. Detta i stället för att som tidigare drifta och underhålla IT-system inom den egna organisationen. Syftet med denna granskning har varit att bedöma hurvida den interna kontrollen kopplat till IT-området är tydlig och uppfyller verksamheternas krav på ändamålsenlighet, med utgångspunkt från de förändringar som gjorts avseende IT-driften. Vidare bedöms huruvida roller och ansvar med avseende på IT-säkerhet är ändamålsenlig.

Haninge kommun har i perioder haft vissa problem med belastningsattacker mot kommunens IT-nätverk. Detta har inte inneburit att faktiska intrång har gjorts eller att väsentliga datamängder gått förlorade utan mer haft konsekvenser på kapacitet och funktionalitet på vissa områden. Kommunen har med anledning av detta under föregående år vidtagit åtgärder för att komma tillrätta med problemen, vilket inneburit extra kostnader i viss utstreckning.

Det pågår ett arbete inom kommunen rörande flera områden med avseende på hantering av IT. Projekt har initierats när det gäller att inventera behov av IT-kapacitet inför kommande år (kartläggning av investeringsbehov) samt även projekt för att tydliggöra faktiska kostnader för IT. Detta bedömer vi vara ändamålseniga åtgärder och högst relevanta.

Vår bedömning är dock att kommunen bör prioritera arbetet med att arbeta fram relevanta och ändamålsenliga styrdokument med avseende på kommunens arbete med IT. Detta gäller inte minst när det handlar om att tydliggörande den strategiska rollen för IT inom kommunens olika verksamheter samt hur detta ska återspeglas i strukturen för intern kontroll.

Med anledning av de iakttagelser som gjorts inom ramen för granskningen lämnas följande rekommendationer:

Rekommendationer

- ✓ Kommunen bör tydliggöra hur IT ska integreras på ett ändamålsenligt sätt i kommunens övergripande struktur för intern kontroll.
- ✓ Kommunen rekommenderas att fastställa och tydliggöra en kommunövergripande IT-strategi samt tydliga riktlinjer när det gäller informationssäkerhet.
- ✓ Tydliggör roller och ansvar mellan den centrala IT-funktionen och respektive systemägare ute i verksamheterna.
- ✓ Kommunen bör överväga att tydliggöra den strategika tyngden när det gäller hantering av IT-området samt hur detta ska återspeglas i kommunens ledningsstruktur.

2. Inledning

2.1. Bakgrund

All verksamhet blir i allt högre grad beroende av informationsteknologi (IT) i olika former. Verksamheter som vi tidigare inte förknippade med nyttjande av IT-verktyg och IT-stöd blir allt mer beroende av fungerande IT-system. Detta gäller i allra högsta grad samhällskritisk verksamhet som bedrivs i kommuner. IT har även blivit en strategisk resurs för ett uppnå ändamålsenlighet samt effektivitet inom de verksamheter där kommunen bedriver verksamheter.

En verksamhets beroende av IT medför dock risker, om än i olika grad. Ett exempel är den ökade sårbarheten vid olika former av driftstörningar. Det är därför väsentligt att ta reda på hur IT-säkerhetsarbetet hanteras. Utifrån vilka regler och anvisningar hanteras säkerhetsarbetet och hur sker kommunikationen och underhållet av använda system?

Kommunens revisorer har i sin risk- och väsentlighetsanalys bedömt att den interna kontrollen kopplat till IT-strukturen är av väsentlighet att granska, i syfte att bedöma huruvida den interna kontrollen är tillräcklig. Detta inte minst ur ett strategiskt perspektiv. År 2010 genomfördes en betydande förändring av Haninge kommuns IT-arbete då drift av IT-system lades ut på extern leverantör, i stället för att som tidigare drifta och underhålla IT-system inom den egna organisationen. Denna granskning följer upp aktuell status för kommunens IT-arbete på en övergripande nivå.

2.2. Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om den interna kontrollen kopplat till IT-strukturen är tydlig och uppfyller verksamheternas krav på ändamålsenlighet. Vidare bedöms huruvida roller och ansvar med avseende på IT-säkerhet är ändamålsenligt.

Följande revisionsfrågor har utgjort utgångspunkt för granskningen:

- ✓ Hur säkerställs informationssäkerhet samt funktionalitet och säkerhet i de IT-system som kommunen använder?
- ✓ Är ansvarsfördelningen med avseende på IT-säkerhet tydlig?
- ✓ Finns tydliga styrdokument (policy, riktlinjer etc.) och följs efterlevnaden av dessa upp regelbundet?
- ✓ Genomförs regelbundna riskanalyser med avseende på IT-området? I så fall, hur ofta?
- ✓ Görs uppföljningar av IT-kostnader?
- ✓ Hur arbetar kommunen med IT-konsulter, i synnerhet upphandling, styrning och uppföljning av IT-tjänster?

Granskningen innebär inte att några säkerhets tester av systemen el. dylikt har genomförts.

2.3. Ansvarig nämnd

Granskningen avser kommunstyrelsen, samt övriga nämnder.

2.4. Granskningens genomförande

Granskningen har baserats på intervjuer samt dokumentstudier av för granskningen relevanta dokument.

3. Kommunens organisation med avseende på IT

3.1. Övergripande struktur avseende drift av IT inom kommunen

Kommunens revisioner genomförde år 2010 en granskning, med specifik inriktning mot kommunens arbete kopplat till IT-och informationssäkerhet. Sedan den granskningens genomförde har kommunens arbete och organisation kring IT väsentligen förändrats, varför en uppföljning av just den granskningen inte är av omedelbar relevans. De iakttagelser och rekommendationer som den granskningen föranledde var inriktade på säkerhetsaspekter som behörighetshantering, fysiskt säkerhet av serverutrustning, kontinuitetsplanering etc. Hanteringen av dessa riskområden har i hög utsträckning förts över till den externa leverantör (Tieto) som numer hanterar driften av kommunens IT-plattform. Rutiner för kontroll av behörigheter till väsentliga system, rutiner för tagande av backuper av datamängder, avbrottshantering etc. ligger inom ramen för avtalet med den externa leverantören Tieto.

De risker som revisionen identifierat i samband med denna granskning har mer att göra med kommunens strategiska arbete med IT samt kopplingen mellan IT och intern kontroll på en övergripande nivå.

Haninge kommun har sedan år 2010 avtal med extern part (Tieto) som driftar kommunens IT-plattform samt därmed även större och väsentliga IT-system. Avtalet med Tieto har ingåtts (upphandlats) tillsammans med Nynäshamns kommun samt Södertälje kommun. Inom ramen för avtalet med den externa leverantören finns former för fysisk och logisk säkerhet.

I samband med denna granskning har det framkommit information om att kommunen i perioder haft vissa problem med belastningsattacker mot kommunens IT-nätverk, främst inom utbildningsförvaltningen. Detta har inte inneburit att faktiska intrång har gjorts utan mer haft konsekvenser på kapaciteten och funktionaliteten på vissa områden. Kommunen har med anledning av detta vidtagit åtgärder för att komma tillrätta med dessa problem, vilket inneburit extra kostnader i viss utstreckning.

3.2. Pågående förändringsarbete med avseende på hantering av IT

Sedan driften av kommunens IT lades ut på extern leverantör har kommunens egen IT-organisation varit inriktad på beställar- och kravställning samt uppföljning. Vidare har kommunens centrala IT-enhet arbetat med IT-relaterade projekt av olika slag. Enheten är uppdelad i ett beställarkontor samt ett programkontor vilka beskrivs i kommande avsnitt. Ny IT-chef tillträdde under början av hösten 2014. Den nytillträdda IT-chefen har en ambition att till den centrala IT-enheten rekrytera viss ny kompetens som kommunen inte tidigare har haft, detta i syfte att möjliggöra en mer strategisk inriktning på kommunens IT-arbete. Vidare pågår det inom enheten projekt med att arbeta fram verktyg för att på ett tydligare sätt inventera behov av IT-stöd inför framtiden samt möjliggöra tydligare former för uppföljning, bland att med avseende på IT relaterade

kostnader. I detta arbete ligger också att hitta en tydligare och mer transparent ”finansieringsmodell” inom kommunen. Med detta avses en modell för fördelning av kostnader mellan verksamheterna där den huvudsakliga fördelningsfaktorn ska utgöras av faktiskt kapacitets- och tjänsteutnyttjande.

4. Bedömning utifrån revisionsfrågorna

I de följande avsnitten besvaras revisionsfrågorna samt att bedömningar lämnas.

4.1. Hur säkerställs informationssäkerhet samt funktionalitet och säkerhet i de väsentliga IT-system som kommunen använder?

Driften av kommunens väsentliga IT-system sker av extern part sedan år 2010. Hårdvara, d.v.s. datorer och arbetsstationer, leasas av kommunen. Ett bakomliggande syfte med att låta extern part drifta kommunens IT-plattform har varit att minska risker för driftsproblem samt andra risker kopplade till IT-säkerhet. Den externa leverantör som kommunen, tillsammans med Nynäshamns kommun och Södertälje kommun, har ingått avtal med bedöms ha både kapacitet och specifik kompetens inom väsentliga områden och kan leverera efterfrågade tjänster på ett mer kostnadseffektivt sätt än vad som skulle vara möjligt om kommunen driftade all IT på egen hand. Det leveransavtal som ingåtts med den externa leverantören omfattar både drift och informationssäkerhet, bland annat rörande behörighetskontroller, tagande av backuper etc.

Ytterligare en viktig aspekt på att låta en extern part drifta kommunens IT är att inför framtiden säkerställa tillgång till teknisk utveckling där kostnader kan ”delas” med flera andra kommuner, med likartade behov.

Kommunens IT-enhet har regelbundna möten med leverantören i syfte att säkerställa att problem och synpunkter fångas upp på ett tidigt stadium och att relevanta åtgärder sätts i vid problem.

Vår övergripande bedömning är att det finns förutsättningar för en ändamålsenlig driftssäkerhet med avseende på kommunens IT-plattform. Detta med utgångspunkt från det driftsavtal kommunen har med extern leverantör. Upplägget med att låta extern part drifta kommunens IT-plattform skapar förutsättningar för att kommunen kan koncentrera sina resurser på utvecklingsprojekt, kravställning och uppföljning.

Under senare tid har det genomförts projekt tillsammans med den externa leverantören för att fysiskt föra över serverkapacitet från kommunen till extern part. Också det ett sätt att utveckla och säkerställa en kostnadseffektiv drift. Det noteras att det inom kommunen pågår flera olika utvecklingsprojekt inom IT-området, bland annat när det gäller att inventera och sammanställa IT-relaterade investeringsbehov inför framtiden. Revisionen ser positivt på denna typ av utvecklingsprojekt och ämnar följa upp dessa framöver, då dessa är av strategisk betydelse i kommunens verksamhetsutveckling, inom flera områden.

4.2. Är ansvarsfördelningen för kommunens IT-hantering tydlig?

Inom kommunstyrelseförvaltningen finns en särskild IT-enhet BIT (Beställarenehet IT), vilken främst utgör en beställarfunktion när det gäller drift och underhåll av väsentliga IT-system. Vidare sker inom enheten uppföljning och kontroll av erhållna tjänster samt bedrivande av IT-relaterade projekt med strategisk inriktning. IT-enheten sorterar organisatoriskt under kommunstyrelseförvaltningen med personaldirektören som har

det övergripande ansvaret. Den centrala IT-enheten leds av en IT-chef, som tillträdde under hösten 2014, som rapporter till kommunens personaldirektör. IT-enheten är uppdelad i ett så kallat ”driftskontor”, med det pratiska ansvaret för kravställning och uppföljning av driftsavtalet med den externa leverantören, samt ett ”programkontor” med inriktning på processer, bedrivande av utvecklingsprojekt etc. IT-enheten har totalt ca 13 anställda, inklusive IT-chefen. Inom enheten råder en tydlig roll- och ansvarsfördelning.

Det noteras således att det i kommundirektörens ledningsgrupp inte finns specifik IT-kompetens representerad. Ur ett strategiskt perspektiv kan detta utgöra en risk då IT, på ett tydligt sätt påverkar och genomsyrar alla de olika verksamheter som bedrivs inom kommunen, om än på olika sätt.

I syfte att möjliggöra ett tydligare utvecklingsarbete med avseende på IT har det beslutats inom kommunen att tillsätta tjänster som ”IT-samordnare” inom respektive fackförvaltning. Syftet är att skapa tydligare och effektivare kontaktytor med respektive verksamhet samt därigenom möjliggöra strategiskt utvecklingsarbete. Rekryteringar till dessa tjänster har påbörjats, i vart fall när det gäller utbildningsförvaltningen. Vår bedömning är att det är positivt att IT-samordnare tillsätts samt att dessa får en tydlig roll som en samverkande länk mellan verksamheterna och den centrala IT-funktionen. Detta möjliggör att verksamheternas behov fångas upp på ett tydligare sätt samt att uppföljning och kontroll effektiviseras.

När det gäller roller och ansvar är det av väsentlighet att notera att det för väsentliga IT-system finns systemägare utsedda. Vår granskning har dock visat att innebörden av det faktiska systemägarskapet inte alltid utövas på ett tydligt sätt vilket utgör en brist. Vår bedömning är således att systemägarskapet för använda system bör tydliggöras, vilket är av betydelse ur ett internt kontrollperspektiv. Vidare är det revisionens bedömning att det bör övervägas att ytterligare lyfta IT-områdets strategiska betydelse genom att ha specifik IT-kompetens representerad i den högsta kommunledningen.

4.3. Finns tydliga styrdokument (policy, riktlinjer etc.) och följs efterlevnaden av dessa upp regelbundet?

Inom kommunstyrelseförvaltningen har det utarbetats styrdokument med avseende på IT. De styrande dokumenteten inom IT-området utgörs av IT-strategi samt informationssäkerhetspolicy. Vid tidpunkten för denna granskning var styrdokumenten inte slutligt fasställda, varför vi inte har tagit del av dessa. I kommunstyrelsens plan för intern kontroll berörs IT-området endast kortfattat.

Vad gäller den kontinuerliga driften av kommunens IT utgör avtalet, med dess tillhörande bilagor, med Tieto det huvudsakliga styrdokumentet. Då huvudavtalet löper under en relativt lång tidsperiod, åren 2010 till 2017, sker ett visst utvecklingsarbete kring avtalet och hur det ska anpassas på ett tydligare sätt till just Haninge kommuns behöv. För närvarande sker utveckling av en så kallad tjänstekatalog som Haninge kommun kan avropa från och hur denna katalog ska vara prissatt. Syftet med att övergå till en modell med avrop av ett antal definierade tjänster är att få ett bättre grepp om det faktiska behovet ute i verksamheterna och därigenom synliggöra resursåtgång och kostnader på ett tydligare sätt.

Inom IT-enheten finns det styrdokument som handlingsplaner, nedbrutna mål etc.

Vår bedömning är att det är av väsentlig betydelse att kommunstyrelsen prioriterar arbetet med att fastställa och förankra en tydlig och kommunövergripande IT-strategi samt därtill hörande informationssäkerhetspolicy. Detta är av vikt då IT i allt större

utsträckning utgör en strategisk del inom de verksamheter kommunens bedriver. Vidare utgör tydliga styrdokument en viktig del när det gäller att tydliggöra roller och ansvar samt åtagande ur ett internt kontrollperspektiv.

4.4. Genomförs regelbundna riskanalyser av IT-systemen? I så fall, hur ofta?

Inom Haninge kommun upprättas inga specifika eller övergripande riskanalyser med avseende på IT och informationssäkerhet. Dock noteras att IT finns med i kommunstyrelsens plan för intern kontoroll där framför allt driftssäkerhet samt säkring av datamängder (backup) finns med som kontrollmoment under året. Skrivningarna i planen för intern kontroll samt därtill hörande risk- och väsentlighetsanalys är av en mycket kortfattad och övergripande karaktär.

När det gäller risker kopplat till den dagliga driften av kommunens IT sker riskanalyser inom ramen för avtalet med den externa leverantören. I viss utsträckning dokumenteras detta. I intervjuer har framkommit att risker, av olika slag, diskuteras på ett regelbundet sätt inom den centrala IT-enheten.

4.5. Görs uppföljningar av IT-kostnader?

Inom ramen för kommunens ekonomistyrning sker uppföljning av verksamhetskostnader av olika slag och på olika nivåer, också med avseende på IT. Kommunövergripande och gemensamma kostnader allokeras via fördelningsnycklar, dock inte med utgångpunkt från faktiskt kapacitetsutnyttjande vilket vore önskvärt. Som nämnts tidigare pågår ett arbete med att ta fram en prissatt tjänstekatalog. Detta i syfte att tydligöra faktiska IT-kostnader för kommunens olika verksamheter samt hur dessa ska fördelas.

I samband med mer djupgående kostnadsanalyser har det visat sig att det föreligger svårigheter att fånga och identifiera samtliga kostnader som är relaterade till IT. I viss utstreckning har förvaltningar engagerat extern IT-kompetens av olika slag utan att dessa nödvändigtvis klassas som IT-kostnader. Innebörden är att det är svårt att bedöma i vilken omfattning kommunens IT-kostnader ligger på en ”normal” eller förväntad nivå i jämförelse med andra kommuner.

Svårigheter att identifiera och mäta samtliga IT-relaterade kostader har föranlett IT-enheten att initiera projekt för att på ett tydligare sätt möjliggöra en ändamålsenlig uppföljning av IT-kostnader. Detta är inte minst viktigt ur ett effektivitetsperspektiv. Projektet är pågående i samband med denna granskning. Vår bedömning är att det är positivt att det finns en vilja och ambition att hitta verktyg för att identifiera och synliggöra IT-kostnader på ett sätt som inte är möjligt för närvarande. När arbetet är klart finns förutsättningar för en mer ändamålsenlig ekonomistyrning.

4.6. Hur arbetar kommunen med IT-konsulter, i synnerhet upphandling, styrning och uppföljning av IT-tjänster?

Kommunens huvudsakliga avtal avseende IT-tjänster utgörs av avtalet med Tieto som löper fram till och med år 2017. Avtalet rör drift av kommunens IT-plattform, inklusive telefoni. Utöver detta finns ramavtal inom IT-området avseende vissa specifika tjänster. Det har framkommit i granskningen att förvaltningarna i olika omfattning och i olika situationer använder sig av IT-konsulter. Detta sker emellanåt utan samordning med kommunens centrala IT-enhet. Modellen med att tillsätta IT-samordnare i respektive nämnd är ett sätt att skapa förutsättningar för en bättre samordning och kontroll över de IT-tjänster som köps in. Vår bedömning är att det är positivt att kommunen genomför ett förbättringsarbete inom detta område.

5. Slutsatser och rekommendationer

Vår övergripande bedömning är att det pågår ett positivt och viktigt förändringsarbete inom kommunen med avseende på hantering av IT. De noteringar och rekommendationer som tidigare granskningar renderade i har beaktats på ett rimligt sätt i det avtal som ingåtts med Tieto. Kommunens utmaningar ligger främst i att kunna anpassa organisation och kapacitet när det gäller IT till verksamheternas uppdrag och mål, i en kommun med en kraftig expansionstakt. Med anledning av detta är det väsentligt att kommunen tydliggör den strategiska inriktning när det gäller IT-området samt kopplingen till det övergripande arbetet med intern kontroll. Detta bör vara dokumenterat på ett tydligt sätt i fastställda riktlinjer och styrdokument.

Vår bedömning är att det föreligger en tydlig fördelning av roller- och ansvar på en övergripande nivå. Systemägare finns utsedda för relevanta system, men detta ansvar är inte i samtliga fall förankrat fullt ut i organisationen.

Vidare är det vår bedömning att det strategiska arbetet med IT är av sådan betydelse att detta på ett tydligare sätt bör återspeglas i kommunen ledningsorganisation.

I syfte att ytterligare stärka den interna kontrollen kopplat till IT-området lämnar vi följande rekommendationer till kommunen att beakta:

Rekommendationer

- ✓ Kommunen bör tydliggöra hur IT ska integreras på ett ändamålsenligt sätt i kommunens övergripande struktur för intern kontroll.
- ✓ Kommunen rekommenderas att fastställa och tydliggöra en kommunövergripande IT-strategi samt tydliga riktlinjer när det gäller informationssäkerhet.
- ✓ Tydliggör roller och ansvar mellan den centrala IT-funktionen och respektive systemägare ute i verksamheterna.
- ✓ Kommunen bör överväga att tydliggöra den strategika tyngden när det gäller hantering av IT-området samt hur detta ska återspeglas i kommunens ledningsstruktur.

Stockholm den 6 mars 2015

Johan Perols
Certifierad kommunal revisor