Säters kommun

Revisorerna *2014-11-11*

Kommunstyrelsen
Kommunfullmäktige för kännedom

"IT-verksamheten"

KPMG har av Säters kommuns revisorer fått i uppdrag att bedöma om styrningen av IT-verksamheten inom *IT-enhetens* ansvarsområde är effektiv och ändamålsenlig

Sammanfattningsvis pekar vi på följande utvecklingsområden:

- IT som stöd är idag en förutsättning för att verksamheten i en kommun ska kunna bedrivas kostnadseffektivt. För att IT ska vara en resurs och inte enbart en kostnad krävs en effektiv styrning baserat på korrekta beslutsunderlag av hög kvalitet. Säters kommuns revisorer bedömer att det finns en risk att IT-styrningen inte bidrar till att IT nyttjas på optimalt sätt

- De styrande dokumenten för IT-verksamheten i kommunen är av äldre datum. Det saknas tillämpningsföreskrifter. En dokumenterad formalisering av IT-enhetens (ITE) uppdrag och ansvar saknas. Den formella samordningen med verksamheterna i övrigt saknas även den. Vi uppfattar att ITE styr sin verksamhet efter budget, tradition och hävd.

- Vi rekommenderar att det bildas en tjänstemannagruppering (IT-råd, IT-forum etc.) som har till uppgift att engagera, samordna, rådge och stödja förvaltningarna, likväl som den politiska ledningen, i de IT-relaterade delarna av kommunens verksamhet.

- Det är positivt att kunna notera i förslag till nya policys att informationssäkerhet (i dokumenten angiven som det underordnade IT-säkerhet) är en viktig del i kommunens verksamhet.

- Vi ser mycket positivt på att Säters kommun upprättar ett IT-bokslut årligen

Revisionen begär yttrande över bifogad rapport, senast 2015-02-01.

De förtroendevalda revisorerna i Säters kommun

Enl uppdrag

Bengt Wester

Curt Söderberg

Säters kommun

IT-verksamheten
Revisionsrapport

KPMG AB
11 november 2014
Antal sidor: 9
Bilaga IT-bokslut 2013

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Innehåll

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

1. Sammanfattning

1.1 Bakgrund och syfte

IT som stöd är idag en förutsättning för att verksamheten i en kommun ska kunna bedrivas kostnadseffektivt. För att IT ska vara en resurs och inte enbart en kostnad krävs en effektiv styrning baserat på korrekta beslutsunderlag av hög kvalitet. Säters kommuns revisorer bedömer att det finns en risk att IT-styrningen inte bidrar till att IT nyttjas på optimalt sätt. Syftet med granskningen har varit att bedöma om styrningen av IT-verksamheten inom IT-enhetens ansvarsområde är effektiv och ändamålsenlig.

1.2 Iakttagelser och kommentarer

Från granskningen vill vi särskilt framhålla:

De styrande dokumenten för IT-verksamheten i kommunen är av äldre datum. Det saknas tillämpningsföreskrifter. En dokumenterad formalisering av IT-enhetens (ITE) uppdrag och ansvar saknas. Den formella samordningen med verksamheterna i övrigt saknas även den. Vi uppfattar att ITE styr sin verksamhet efter budget, tradition och hävd. I mitten av oktober 2014 presenterade IT-chefen förslag till nya styrande dokument för kommunstyrelsens arbetsutskott. Dokumenten är enligt uppgift förankrad hos förvaltningscheferna. Vad vi förstår så togs dokumenten och föredragningen emot positivt av KSAU. Det bedöms som möjligt att dokumenten efter mindre justering kan tas upp för beslut kommunstyrelsen innan årets slut.

Det är viktigt, inte enbart för ITE, att tydligt och dokumenterat känna till uppdrag, ansvar och resurser. I förslag till nya policys ges ITE ett sådant ansvar. Till policys krävs tillämpningsföreskrifter. Om kommunens ledningsgrupp inte anses vara rätt forum för att upprätta dessa så rekommenderar vi att det bildas en tjänstemannagruppering (IT-råd, IT-forum etc.) som har till uppgift att engagera, samordna, rådge och stödja förvaltningarna, likväl som den politiska ledningen, i de IT-relaterade delarna av kommunens verksamhet. Vi anser att det är kommunchefen som leder IT-rådets arbete och att chefen för ITE är en medlem som alltid finns med vid alla möten. Vi upplever att ITE genom detta skulle få ett tydligare och konkretare formulerat uppdrag från politik och verksamhetsledning.

ITE är anslagsfinansierad som en del av kommunledningskontoret. Både drift- och investeringsbudget minskas något från 2014 till 2015. Den ambition som framkommer i förslagen till nya policydokument måste även avspegla sig i en budget som möjliggör att definierade mål har en möjlighet att uppnås.

Det är positivt att kunna notera i förslag till nya policys att informationssäkerhet (i dokumenten angiven som det underordnade IT-säkerhet) är en viktig del i kommuns verksamhet. I sammanhanget är det då viktigt att notera att MSB inte längre stöder och utvecklar BITS. Det har i stället ersatts av ett LIS (Ledningssystem för informationssäkerhet).

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Barn- och utbildningsförvaltningen köper tjänster av företag som innebär att personuppgifter hanteras utanför kommunen. Ett personuppgiftsbiträdesavtal har upprättats. Detta är en indikation på att kommunen med noterade förbehåll tillåter att denne att hantera personuppgifter. Det framkommer inte under vilka tekniska förutsättningar kommunen köper tjänsten. När en utomstående aktör tillåts hantera integritetskänslig information är det inte sällan motiverat att kontrollera vad som avtalats förutom vad som tas upp i ett personuppgiftsbiträdesavtal. Vi rekommenderar att avtalet (för tjänsten) kontrolleras i förhållande till vad som framgår av PuL[1] och att det säkerställs att upphandling av denna typ av tjänster sker med stöd av kunnig personal och efterlevande de regler för informationssäkerhet som gäller i kommunen.

[1] Personuppgiftslag (1998:204)

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

2. Bakgrund

Informationsteknologi är ett vitt begrepp som omfattar större och större områden. Allt från det man i vanliga fall tänker sig ingår såsom datorer, programvaror och skrivare till telefoner, passersystem och mycket annat. Informationsteknologi är därmed inte bara ett brett område utan också ett komplext område som får ett stort genomslag genom höga direkta kostnader i form av investeringar men också genom stora besparingar genom att bidra till ett effektivt arbetssätt. För att nå något som brukar vara ett mål nämligen att IT ska vara en resurs och inte en kostnad krävs en effektiv styrning baserat på korrekta beslutsunderlag av hög kvalitet.

Säters kommuns revisorer bedömer att det finns en risk att IT-styrningen inte bidrar till, vilket är väsentligt, att IT nyttjas på optimalt sätt i organisationen och genomför därför denna granskning som en del av den ansvarsutövande granskningen för år 2014.

3. Syfte

Syftet med granskningen har varit att bedöma om styrningen av IT-verksamheten inom *IT-enhetens* ansvarsområde är effektiv och ändamålsenlig. Vi har därför granskat:

- Styrningen av IT-verksamheten.
- Vilka styrande dokument i form av policys och riktlinjer som finns.
- Hur roller och ansvar fördelade.
- Vem/vilka som har rätt att teckna avtal.
- Hur IT-enheten finansieras.
- Hur kommunens gemensamma IT-infrastruktur är utformad.
- Hur övriga verksamheter uppfattar IT-enhetens stöd och support, samt inköp, installation och underhåll.

4. Avgränsning

Granskningen omfattar kommunens *IT-enhet*. Specialsystem och speciallösningar som omfattar en eller ett fåtal verksamheter berörs inte av denna granskning. Vi har i denna granskning inte granskat säkerhetsaspekterna speciellt utom om vi iakttagit uppenbara säkerhetsrisker. De kommunala bolagen och eventuella utkontrakteringsparteners omfattats inte av granskningen.

5. Ansvarig styrelse

Granskningen avser kommunstyrelsen.

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

6. Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med IT-chefen. Rapporten är saklighetsgranskad av densamma.

7. Granskningsnoteringar

Vi använder punktlistan under avsnittet syfte som indelning av våra noteringar. I respektive avsnitt redovisar vi iakttagelser och våra kommentarer.

7.1 Styrningen av IT-verksamheten.

IT-verksamheten i sin helhet styrs enligt de dokument som redovisas i avsnittet 7.2 nedan.

IT-enheten är ett av fem kommunledningskontor. Dessa är kommunstyrelsens förvaltning och bildades 2013-01-01 i samband med en omorganisation. Kommunchefen fungerar som förvaltningschef.

Vi kan inte finna att en dokumenterad uppdrags- och ansvarsbeskrivning för IT-enheten upprättats och kommunicerats. Enheten själv har i avsaknad av en sådan inte själva dokumenterat hur de uppfattar sitt uppdrag och ansvar. Vi kommenterar detta i avsnittet 7.2 nedan.

7.2 Vilka styrande dokument i form av policys[2] och riktlinjer som finns.

Det centrala dokumentet vid granskningstillfället är IT-strategin. Dokumentet antogs 1999 och finns nu i en reviderad version antagen av kommunfullmäktige (KF) 2005-01-24. Det finns inga tillämpningsföreskrifter till strategin.

Vi uppfattar att IT-enheten (ITE) i övrigt styr sin verksamhet efter tradition och hävd. ITE upplever att man informellt har det inflytande som behövs för att dag för dag stödja övrig verksamhet. Den formella samordningen med verksamheterna saknar man dock. Dagens planeringsmöten på systemförvaltarnivån anses behöva kompletteras med regelbundet återkommande samordningar med ledningen av förvaltningarna. Endast planering och mandat baserat på budget anses inte som ändamålsmässiga styrmedel för att nå ett effektivt utnyttjande av de gemensamma IT-resurserna.

ITE jobbar för egen del efter en årsplan innehållande en planering av de egna resurserna. Det läggs särskild vikt vid planeringen av projekt som löper över längre tid.

ITE upprättar sedan flera år tillbaks årligen ett dokument benämnt IT-bokslut (ITB). Av ITB: s sju sidor för 2013 framgår följande:

[2] En policy enligt vårt synsätt består av ett policydokument - fullmäktiges beslutar om att något skall följas/uppnås. Till det läggs tillämpningsföreskrifterna. Vi väljer att kalla den första för riktlinjer vilka utfärdas av verksamhetsansvariga på kommunövergripande nivå. Av dem framgår vad som ska göras. För ytterligare detaljer där ansvaret följer ansvaret i linjen kommer anvisningar som anger på vilket sätt. I instruktioner beskrivs sedan när och av vem.

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

- En inledande beskrivning av ITE
- Resultatet av en årligen återkommande enkät av hur övrig verksamhet uppfattar ITE och den verksamhet de bedriver.
- Ett statistikavsnitt som redovisar hur och var kommunens hårdvara används.
- Information om de verksamhetssystem som finns med tyngdpunkt på de som är mest viktiga för verksamheten. I avsnittet redovisas även att respektive verksamhetsansvariga ytterst äger och ansvarar för sina system.
- Infrastrukturen i kommunen beskrivs.
- Särskilda händelser under året redovisas under rubriker som:
    - Samarbete.
    - Uppdatering av system.
    - Större projekt.
    - Utbildningar.
    - Incidenter.
- Kostnadsredovisning.
- Planering för kommande år uppdelat på systemuppdatering, nya system/programvara och ett avsnitt för övrigt.

Vår granskningsnoteringar i avsnitten nedan hämtar flera av sina iakttagelser från ITB.

I mitten av oktober 2014 presenterade IT-chefen ett förslag till nya styrande dokument för kommunstyrelsens arbetsutskott (KSAU). Dokumenten är enligt uppgift förankrad hos förvaltningscheferna. Vad vi förstår så togs dokumenten och föredragningen emot positivt av KSAU. Det bedöms som möjligt att dokumenten efter mindre justering kan tas upp för beslut kommunstyrelsen innan årets slut.

IT-policyn anger underlag och anvisningar för kort- och långsiktiga IT-investeringar samt skall följa e-policyn intensioner. Dokumentet anger inriktningen för ansvar, ledning och genomförande. Kommunstyrelsen samt nämnders och styrelsers förvaltningar, kommuns ledningsgrupp och IT-enhets roller och ansvar beskrivs. Genomförandebeskrivningen inriktar sig mot tillgänglighet, säkerhet och effektivitet. e-Policyn i sin tur anger även den inriktningen för ansvar och ledning med roller och ansvar. Med utgångspunkt i mål för e-demokrati, e-tjänster och e-förvaltning redovisas övergripande hur utvecklingen skall ske.

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Kommentar

Det är viktigt, inte enbart för ITE, att tydligt och dokumenterat känna till uppdrag, ansvar och resurser. I förslag till nya policys ges ITE ett sådant ansvar. Policys anger att något skall göras/uppnås, mål definieras. Policys behöver konkretiseras i tillämpningsföreskrifter vilka anger vad som skall göras. Om kommunens ledningsgrupp inte anses vara rätt forum för att upprätta dessa så rekommenderar vi att det bildas en tjänstemannagruppering (IT-råd, IT-forum etc.) som har till uppgift att engagera, samordna, rådge och stödja förvaltningarna, likväl som den politiska ledningen, i de IT-relaterade delarna av kommunens verksamhet. Vi anser att det är kommunchefen som leder IT-rådets arbete och att chefen för ITE är en medlem som alltid finns med vid alla möten. Vi upplever att ITE genom detta skulle få ett tydligare och konkretare formulerat uppdrag från politik och verksamhetsledning. Inte bara ITE: s egen verksamhet skulle vinna på detta utan även all verksamhet som stöds av IT.

IT-rådet skulle initialt kunna inrikta sig mot tre områden:

- Strategi – proaktiv styrning för utveckling som svarar mot verksamheternas behov.
- Säkerhet – skapa medvetenhet, öka tillförlitligheten och upparbeta robusta rutiner.
- Resultat – överenskomna leveransnivåer som kan följas upp och värderas.

Det bör framåt i tiden aldrig råda någon tvekan om att det är IT-rådets beslut som gäller i IT-frågor.

IT-bokslutet är en informativ och faktafylld sammanfattning av ett "IT-år". Vi rekommendera att det årligen studeras av alla verksamheter. Inte minst av den anledningen bilägger vi 2013 års ITB till denna rapport.

7.3 Hur roller och ansvar är fördelade

På ITE finns sammanlagt fem medarbetare. En chef, en teknikansvarig samt tre tekniker. Fyra stycken delar roterande för bemanningen av ITE: s supportfunktion. Av vad vi förstår så anser sig ITE inte underbemannad.

7.4 Vem/vilka som har rätt att teckna avtal.

ITE utför upphandling och tecknar avtal inom delegationsordningen och budget vilket innebär att större investeringar alltid skall godkännas av överordnad. För ITE: s del innebär det kommunchefen.

ITE ansvarar för och utför upphandling och inköp av hårdvara förutom smarta telefoner vilket är kansliets uppgift. Skrivare leasas. Att all teknikapparatur fungerar tillsammans och kan kommunicera är dock ITE: s ansvar. ITE ansvarar för inköp av system och programbehov för egna enhetens och kommunens allmänna behov. System och program för enskilda verksamheters behov är respektive förvaltnings ansvar. Även här har ITE ansvar för att systemen fungerar rent tekniskt.

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Kommentar

Som en del av det uttryckta behovet om formalisering av ITE: roll och ansvar är det viktigt att även detta område kommer med.

7.5 Hur IT-enheten finansieras.

ITE är anslagsfinansierad som en del av kommunledningskontoret. En behovskalkyl görs inför att en budgetram fastställs. Driftbudgeten för 2014 var drygt 8 MSEK och investeringarna uppgick till inte fullt 1,5 MSEK. För 2015 förväntas utrymmet i båda budgetarna minska något.

Kommentar

Den ambition som framkommer i förslagen till nya policydokument måste även avspegla sig i en budget.

7.6 Utformningen av kommunens gemensamma IT-infrastruktur

Kommunens verksamheter är sammankopplade i ett nätverk. Den ökande användningen av bärbar utrustning innebär att behovet för Wi-Fi ökar. Under 2013 fanns möjligheten till trådlös uppkoppling på alla skolor och flertalet förskolor. Under 2014 har utbyggnaden av trådlösa nätverk fortsatt. Alla användare har tillgång till e-post och extern likväl som intern webb.

ITE köper kommunikationsmöjlighet genom svartfiber[3]. Även Telias och Dala Energis nät används för kommunikation över längre avstånd. Kommunikation gör det möjligt för samnyttjande av GIS- och PA-system med Falu kommun. Säter tillsammans med övriga dalakommuner är tekniskt anslutna till samma telefonväxel.

Kommentar

Skall detta fortsätta att fungera och även möta de behov som målområdena i e-Policyn redovisar krävs även här en formalisering. Inte minst för att allokera medel och tydligt kommunicera ansvar.

7.7 Hur övriga verksamheter uppfattar IT-enhetens stöd och support, samt inköp, installation och underhåll

Under 2013 genomfördes en enkät med målsättningen att få användarnas synpunkter på och förslag till ITE: s arbete. Cirka 60 svar erhölls. Svaren på frågorna var genomgående positiva. Av svaren kunde utläsas att support och bemötande kunde förbättras. Av svaren kunde även utläsas att utrustningen som finns tillgänglig "är till belåtenhet". Det framkommer dock att det är viktigt att ITE följer utvecklingen av både hård- och mjukvara.

[3] Svartfiber är en fiberkabel för sändare och mottagare som kan ägas av privata aktörer eller av en allmännytta. Utrustningen som ansluts i ändarna ägs av den som hyr svartfibern. Svartfiber erbjuder möjligheten för teleoperatörer att ha gemensam infrastruktur, som ett alternativ till att varje operatör lägger ut sin egen fiber.

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Kommentar

Det är lovvärt att återkommande fråga de som är beroende av ITE: s arbete om vad de tycker om hur de lyckas. Överväg en ytterligare ansträngning för att få fler svar från verksamheten. Ett representativt svar från verksamheten är ett inte oväsentligt styrmedel.

7.8 Informationssäkerhet i allmänhet och molntjänster i synnerhet.

Säkerhet är avgränsat att *inte* ingå i granskningen men vi vill ändå nämna att i förslag till IT-policy tydligt anges att:

- IT-säkerhet är en viktig del i kommunens verksamhet.
- MSB[4]: s basnivå för IT-säkerhet (BITS[5]) ska gälla som ramverk för kommunen.
- ITE "utgår från överenskommelser med verksamheten om vilka avbrottstider som kan godkännas innan kommunen lider skada."

Det framkommer under intervju att Barn- och utbildningsförvaltningen använder en lärplattform[6] från Infomentor[7]. Enligt uppgift har det tecknats ett personuppgiftsbiträdesavtal med leverantören. Detta är en indikation på att kommunen med noterade förbehåll tillåter att denne hanterar personuppgifter. Det framkommer inte under vilka tekniska förutsättningar kommunen köper tjänsten.

Kommentar

Det är positivt att kunna notera i förslag till nya policys att informationssäkerhet (i dokumenten angiven som det underordnade IT-säkerhet) är en viktig del i kommuns verksamhet. I sammanhanget är det då viktigt att notera att MSB inte längre stöder och utvecklar BITS. Det har i stället ersatts av ett LIS (Ledningssystem för informationssäkerhet).

När en utomstående aktör tillåts hantera integritetskänslig information är det inte sällan motiverat att kontrollera vad som avtalats förutom vad som tas upp i ett personuppgiftsbiträdesavtal. Kommer leverantören att ange, använda sig av och ansvara för underleverantörer? Om personuppgifter ska hanteras krävs personuppgiftsbiträdesavtal även med underleverantörer. Var kommer information-

[4] Myndigheten för Samhällsskydd och Beredskap

[5] BITS stöds inte längre av MSB. Den som tidigare har arbetat enligt BITS kan dock oftast använda det befintliga arbetet som en viktig utgångspunkt i det fortsatta arbetet. Detta speciellt när det gäller utformningen av skydd för specifika informationssystem.

[6] Wikipedias förklaring av lärplattform: En utbildningsplattform, som i allt högre grad används som komplement till traditionell undervisning, för e-lärande. Den kan beskrivas som ett virtuellt klassrum där kursdeltagare och lärare för en specifik kurs kan kommunicera säkert med varandra, och utbyta lösenordsskyddade dokument. Lärplattformen hanterar kursuppföljning och kursadministration, exempelvis resultatlistor, automaträttade prov, digitalt kursinnehåll i exempelvis text- och videoformat och inlämningskorgar för redovisningsuppgifter. Den kan även hantera individuella utbildningsplaner, inrapportering av närvaro och skriftliga omdömen.

[7] Enligt Infomentors hemsida ägnar sig företaget åt skolutveckling och är specialister på skolans processer, kommunikation och kvalitetsarbete. De erbjuder fortbildning och en webbaserad lärplattform för skolan.

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

en att lagras? Var kommer information att bearbetas? När personuppgifter ska hanteras är huvudregeln att lagringen måste ske i ett land inom EU/EES-området. Det finns leverantörer som skiljer mellan lagring och bearbetning, så även om de garanterar att lagringen sker inom EU/EES kan de ändå bearbeta den utanför. Är det inte tydligt klarlagt var lagring och bearbetning sker kan det strida mot reglerna i PuL[8], där lagring och bearbetning båda faller inom det övergripande begreppet "behandling" av personuppgifter. Vidare, vem har rätt att få åtkomst till informationen? En grundförutsättning är att det tydligt regleras att kommunen "äger" informationen både under avtalstiden men även efter avslut. Leverantören ska inte ha rätt att utifrån sina egna behov disponera över informationen. Att man kan få ut logginformation så att det kan kontrolleras vem som har haft åtkomst till informationen är en viktig del i att över tid veta hur den hanteras av leverantören. Sist men inte minst, efterlever avtalet de regler om säkerhet för information som kommunen själva beslutat om?

Vi rekommenderar att avtalet (för tjänsten) kontrolleras i förhållande till vad som sagts ovan och att det säkerställs att upphandling av denna typ av tjänster sker med stöd av kunnig personal och efterlevande de regler för informationssäkerhet som gäller i kommunen.

KPMG, dag som ovan

Lars Anteskog
Projektansvarig

Mats Lundberg
Kundansvarig

[8] Personuppgiftslag (1998:204)

© 2014 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.