Granskning av kommunens IT-verksamhet

Revisionsrapport

Tranås kommun

KPMG AB

2018-03-06

Antal sidor 11

Innehållsförteckning

1 Inledning/bakgrund

Vi har av Tranås kommuns fått i uppdrag att genomföra en granskning av kommunens IT-verksamhet. Uppdraget ingår i revisionsplanen för år 2017.

1.1 Syfte och revisionsfråga

I granskningen ingår att bedöma följande övergripande frågor:

- Hur är kommunens IT-verksamhet organiserad?
- Hur är ansvarsfördelning reglerad mellan styrelse och nämnder?
- Hur fungerar kommunikation mellan centrala IT-avdelningen och olika verksamheter?
- Hur regleras inköp av utrustning och olika system?
- Hur harmoniserar olika system med varandra?
- Tillgodoses verksamheternas önskemål på olika system?
- Vem har helhetssyn på kapacitetsutnyttjandet avseende de olika systemen?
- Hur fungerar konsultstödet till de olika systemen?
- Hur är ansvaret för IT-säkerheten reglerat?
- Vilka kontroller kopplat till IT-säkerhet genomförs?
- Är IT-säkerhetsplaner och annan dokumentation uppdaterade?
- Vilka resurser (ekonomiska och personella) finns för att säkerställa IT-verksamheten?

1.2 Avgränsningar

Granskningen avser kommuns IT-verksamhet om lyder under kommunstyrelsen.

1.3 Revisionskriterier

Vi har bedömt om rutinerna/verksamheten uppfyller

- Lokala föreskrifter och rutiner.

1.4 Ansvarig nämnd

Kommunstyrelsen

1.5 Projektorganisation

Granskningen har utförts av Viktoria Bernstam, revisor/juridisk sakkunnig med Kristian Gunnarsson, kundansvarig som kvalitetssäkrare.

1.6 Metod

Studium och genomgång av relevanta styrdokument och beslutsunderlag.
Intervjuer har genomförts med IT-chefen, kommunstyrelsens ordförande och kommundirektören.

Rapporten har faktagranskats av IT-chefen samt kommundirektören.

2 Organisation och resurser

Iakttagelser

Data- och serviceavdelningen är en del av kommunledningsförvaltningen och lyder under kommunstyrelsen. Avdelningen består av en dataenhet och en serviceenhet. Serviceenheten i sin tur består av reception, vaktmästeri och post samt kommunarkivet.

Dataenheten består av IT-drift, Telefoni-drift, IT-kommunikation, IT-support, Beställning, Ärendekoordinering och Servicedesk. Dataenhetens bemanning uppgår till 9 tjänster vid tid för granskningen. Av intervju med chefen för data- och serviceavdelningen framgår att bemanningen kommer att utökas till 10 tjänster under mars/april månad, där en driftadministratör kommer att anställas.

Dataenheten har en driftbudget på ca 11,5 mnkr, (serviceenheten har exkluderats i syfte att få fram en rättvis ekonomisk bild). Budgeten bedöms enligt professionen som tillräcklig utifrån dagens behov och krav.

Kommentarer

Personella samt ekonomiska resurser är viktiga faktorer för bl.a. en sårbarhets-bedömning. Av granskningen framkommer att dataenhetens bemanning utökades med

en heltidstjänst för ca ett år sedan i syfte att minimera verksamhetens sårbarhet. Ytterligare utökning kommer att ske under våren med en heltidstjänst.

Idag finns en back-up för respektive funktion. Detta innebär att det finns minst två personer som har kunskap och kompetens inom samma funktionsområde och kan backa upp varandra vid oförutsedda händelser samt ledigheter.

3 Ansvarsfördelning kommunstyrelsen och nämnder

Iakttagelser

Vi har tagit del av riktlinjer avseende ansvarsförhållande för IT-system och informationssäkerhet, fastställd 2013-06-18 med senaste revidering 2017-04-05 av kommunstyrelsen.

Av riktlinjerna framgår att kommunstyrelsen ansvarar för den övergripande styrningen och samordningen av kommunens IT-verksamhet. Kommunstyrelsen har vidare beslutanderätt gällande införande av nya IT-system, anskaffning av IT-utrustning och övriga resurser för IT-verksamheten.

Nämnderna är ansvariga för utvecklingen av de egna administrativa systemen samt är uppdragsgivare för de projekt som berör den egna förvaltningen. Nämnden skall också till kommunens personuppgiftsombud anmäla rättighet att upprätta register och ansvarar för att de personregister som arbetas fram inte strider mot dagens PUL, (personuppgiftslagen), samt dataskyddsförordningen.

Dataskyddsförordningen träder ikraft 25 maj 2018 och ersätter PUL.

Kommentarer

Vi bedömer att det finns dokumenterade riktlinjer som anger, beskriver och särskiljer styrelsens och nämnderna olika ansvarsområden.

Riktlinjerna bör dock revideras inför ikraftträdandet av dataskyddsförordningen, där exempelvis benämningen dataskyddsombud ska ersätta personuppgiftsombud. Av riktlinjens försettblad framgår att revidering kommer att ske först 2021-04-04.
Det är av stor vikt att styrdokument revideras i samma takt som förändrade förutsättningar så som lagstiftning, branschregler, budget mm. i syfte att hålla styrdokumenten àjour.

4 Kommunikation mellan Dataenheten och verksamheterna

Iakttagelser

Av granskningen framgår att kommunikation och samverkan sker bl.a. genom månatliga möten med förvaltningsledningsgruppen, FLG, där förvaltningschefer, avdelningschefer och kommundirektören närvarar.

Ytterligare kommunikation sker genom möten med koncernledningsgruppen, KLG, där också de kommunala bolagsledningarna närvarar. Möten med KLG genomförs fem gånger årligen.

Vidare sker en genomgång med respektive förvaltningsledningsgrupp inför budgetberedningar, där datachefen representerar nämnderna avseende investeringar inom IT.

För att underlätta den interna kommunikationen och IT-stödet har förvaltningarna utsedda kontaktpersoner, (systemansvariga), som hanterar frågor avseende den dagliga driften.

På operativ nivå träffas systemansvariga från respektive förvaltning en gång per månad tillsammans med personal från IT-drift.

Vad gäller större projekt och förändringar som exempelvis dataskyddsförordningen, GDPR (General data protection regulation), har arbetsgrupper med representanter från olika verksamheter skapats.

Kommentarer

Vi bedömer att kommunikationen mellan dataenheten och verksamheterna ligger på en tillfredställande nivå vad gäller strategisk och operativ nivå, utifrån ovanstående mötes- och diskussionsforum.

5 Inköp av IT-system och utrustning samt verksamheternas önskemål

Iakttagelser

Av granskningen framkommer att all IT-system och IT-utrustning som skall införskaffas ska redovisas i den så kallade Digitala agendan, där verksamheternas önskemål avseende årliga IT-investeringar redogörs i samband med budgetberedningen.

Vi har tagit del av dokumenterade rutiner för upphandling och inköp, (fastställd 2017-06-30), samt rutiner för nyanskaffning och införande av verksamhetssystem, (fastställd 2016-06-20 med senaste revidering 2017-06-20).

Av intervju med data- och serviceavdelningens chef framgår att all inköp av IT-system och IT-utrustning går via dataenheten samt upphandlingsenheten som tillsammans med respektive systemansvarig på förvaltningarna hanterar verksamheterna önskemål.

Inför nyanskaffning och införande av verksamhetssystem tillsätts alltid en projektgrupp bestående av en projektansvarig från dataavdelningen samt en projektansvarig från aktuell verksamhet.

Vidare ska en projektplan utformas som beskriver behovet och ändamålet med anskaffningen följt av en systemsäkerhetsanalys som syftar till att kartlägga säkerhetskraven på det nya systemet. En kravspecifikation ska arbetas fram som minst omfattar: integrationskrav, krav på test, tidsplan, personella och ekonomiska resurser, behov av användarutbildning, dokumentbehov så som rutiner, planer checklistor mm.

Kommentarer

Framtagning av en underbyggd kravspecifikation är en grundläggande premiss för nyanskaffning och införande av IT-system och IT-utrustning. Av granskningen framgår att det finns dokumenterade rutiner för anskaffning av IT-system och IT-utrustning. Vi anser att det är en fördel att dataenheten är involverad från start till driftsättning.

6 Systemharmonisering

Iakttagelser

Av intervju med data- och serviceavdelningens chef framgår att styrande ledord vad gäller informationsteknik i kommunen är harmonisering och standardisering. Det ska finnas ett framåtsyftande tänk inför all nyanskaffning av system och utrustning. Ansvaret för att det sker en harmonisering mot befintliga tekniska förutsättningar i samband med uppgraderingar eller inköp ligger på driftenheten.

Ett exempel är användandet av samma behörighetssystem i syfte att undvika flera inloggningar. Detta är möjligt genom en så kallad federerad identitet, dvs. en användaridentitet istället för flera. Förenklat handlar det om flera system men ”en inloggning”.

Av granskningen framkommer att kommunen ör några år sedan hade ca 2000 olika program. Ett aktivt inventeringsarbete avseende programvaror och licenser har lett till att siffran har reducerats till ca 700 idag.

Ytterligare exempel på harmonisering och standardisering är att samtliga verksamheter idag använder samma Office version, där uppgradering av gemensamma programvaror ska ske samtidigt inom kommunens olika verksamheter, dvs. där ingen förvaltning ska ligga före eller efter.

Kommentarer

Det finns en hög ambitionsnivå gällande harmonisering och standardisering av IT-miljön i kommunens verksamheter. Vidare leder den så kallade Digitala agendan till en mer samlad planering och samordning vad gäller just harmonisering. Detta leder i sin tur till en kostnadseffektivitet samt bättre överblick. Vi anser att inventeringar med jämna mellanrum är ytterligare redskap som kan minimera både kostnader och risker.

7 Helhetssyn avseende kapacitetsutnyttjande

Iakttagelser

Vad gäller kapacitetsutnyttjandet är det driftenheten inom data- och serviceavdelningen som tillsammans med respektive systemansvarig ansvarar för en helhetssyn. Driftansvarig hanterar även beräkningar över filtillväxten på kort- och lång sikt.

Vidare är rutinen den att vid särskilda tillfällen lånas kapacitet från en förvaltning till en annan, exempelvis vid nationella prov, där barn- och utbildningsförvaltningen tillfälligt är i behov av en utökad kapacitet.

Det tidigare genomförda inventeringsarbetet har genom elimination av likartade program lett till bl.a. ett bättre kapacitetsutnyttjande.

Kommentarer

Rutiner för kapacitetshantering är en premiss för att kunna bedöma eventuell över- eller underkapacitet. Vi bedömer det som viktigt att det finns tydliga ansvarsroller vad gäller överblick och kontroll av kapacitetsutnyttjande, där driftenheten idag har en central roll.

Det finns vidare en dokumenterad rutin avseende kapacitetshantering för IT-tjänster, dock saknas ett fastställelsedatum för styrdokumentets antagande.

8 Konsultstöd

Iakttagelser

Verksamheterna tecknar egna supportavtal avseende externt konsultstöd. Supportavtal tecknas med respektive leverantör. Dock sköter dataenheten, (drift), dialogen mot leverantören i majoriteten av fall, där förvaltningarna, (systemägarna), anser att rutinen underlättar kommunikationen gentemot leverantören.

Driftenheten står för det dagliga stödet.

Samtliga externa konsulter ska logga in genom kommunens 2-faktorsinloggning, där respektive konsult enbart får tillgång till det system supportavtalet avser.

Kommentarer

Vi kan se en fördel med att kommunikationen gentemot externa konsulter hanteras av data- och serviceavdelningen, där rutinen utöver kommunikationsaspekt och avlastning av förvaltningarna, underlättar även det dagliga stödet.

Vi bedömer vidare att inloggningsrutinerna för de externa konsultstöden är en del av internkontrollarbetet, där rutinen bl.a. bidrar till mer korrekta fakturor.

9 Ansvarsreglering för IT-säkerhet

Iakttagelser

Ansvaret för IT-säkerhet finns reglerat i riktlinjer fastställd av Kommunstyrelsen, (Ks § 119, 2013-06-18 med senaste revidering 2017-04-05, dokument-ID 0797).

Kommunstyrelsen har det övergripande samt yttersta ansvaret för kommunens IT-säkerhet.

Dataenheten ansvarar för det strategiska samt operativa säkerhetsarbetet. Härigenom särskiljs begreppen informationssäkerhet och IT-säkerhet. Det förstnämnda behandlar informationstillgängligheten samt krav på skyddsnivå och konfidentialitet. IT-säkerheten rör de tekniska kraven och säkerhetsåtgärder i form av bl.a. brandväggar, antivirus, kryptering mm. Här ingår även organisatoriska säkerhetsåtgärder som tar sikte på rutiner, regler och planer avseende kommunens säkerhetsarbete.

Vidare har systemägarna, dvs. förvaltningarna med förvaltningscheferna som ytterst ansvariga ett övergripande ansvar för förvaltningssystemen. Systemägarna har också ett ansvar för förvaltningens informations- och IT-säkerhet.

På användarnivå har användarna ett ansvar att efterleva gällande styrdokument avseende informationssäkerhet. I ansvaret ingår rapportering av incidenter.

Av intervju med datachefen framgår att återrapporteringar till kommunstyrelsen sker två gånger årligen.

Kommentarer

Vi bedömer att det finns det finns en tydlig ansvarsreglering avseende informations- och IT-säkerhet utifrån de rutiner som vi har tagit del av. Dock bör kommunstyrelsen undersöka om huruvida efterlevnaden ligger på en tillfredställande nivå inom nämnder och styrelser.

Vi anser att det är av stor vikt med en fungerande samt kontinuerlig kommunikation mellan ansvariga tjänstepersoner och kommunstyrelsen som är ytterst ansvarig.

Av intervjuerna med politiken och professionen framgår att kommunstyrelsen förlitar sig till stor del på datachefen och vederbörandes kompetens. Vi bedömer detta som sårbart, där datachefen håller med denna uppfattning. Datachefen uttrycker att det vore önskvärt med en resurs som kan agera som ”bollplank” vid behov, exempelvis vid juridiska frågor. Inför ikraftträdandet av dataskyddsförordningen kommer kommunstyrelsen att anställa en s.k. dataskyddsombud, där juridisk kunskap är en förutsättning. Detta kan vara en möjlighet, där tjänsten ifråga innebär en naturlig samt nödvändig kommunikation med dataenheten.

Vidare bedömer vi att kommunstyrelsen bör ta fram en plan för kompetensöverföring avseende nyckelpersoner så som datachefen, i syfte att undvika nuvarande sårbarhet samt säkerställa en framtida kompetensförsörjning.

Ett fastställesdatum bör tillföras riktlinjerna för ”informations- och IT-säkerhet, (dokument-ID 0398).

10 Dokumentation

Iakttagelser

Det finns idag ett 40-tal dokument i form av riktlinjer och rutiner. Majoriteten av riktlinjerna och rutinerna har arbetats fram under 2016. Detta beror på övergång till ett nytt ledningssystem under 2016.

Kommentarer

Det finns en del rutiner som har uppdaterats under 2017. Ett flertal rutiner och riktlinjer saknar fastställelsedatum, (bl.a. riktlinjer/rutiner för informations- och IT-säkerhet, kapacitetshanteringsprocess för IT-tjänster, framtagning av kontinuitetsplan för IT-tjänster, informationssäkerhetsklassning, framtagning av uppdaterings- och uppgraderingsplan för IT-tjänster, servicenivåhanteringsprocess för IT-tjänster, beräkning av gemensamma resurser för IT-tjänster).

Vi anser att det är viktig att styrdokumentens aktualitet framgår av dokumentens framsida. Styrdokumentens aktualitet har stor påverkan på tillämpningsgraden ute i verksamheterna. Vidare bör benämningen ”publiceringsdatum” ändras till ”beslutsdatum” följt av ”senaste revidering” i syfte att förtydliga dokumentet giltighet.

Vidare kan alltför många riktlinjer och rutinbeskrivningar leda till en ”dokument-trötthet” ute i verksamheterna som i sin tur riskerar att leda till minskad verkningsgrad och legitimitet. Vi rekommenderar dataenheten att i samband med förbättringsarbetet se över antalet styrdokument för att sondera huruvida det finns möjligheter att reducera samt eliminera likartade styrdokument. Detta i syfte att uppnå en högre implementering och efterlevnad av rutinerna i förvaltningarna.

Av intervju med datachefen framgår att ett förbättringsområde är just efterlevnad av riktlinjer och styrdokument ute i verksamheterna, där det idag ser olika ut. En genomförd GAP-analys, (kortfattad handlar det om identifiering av gapet mellan nuläge och potentialen), bekräftar detta, (se avsnitt 10).

11 Kontroller kopplad till IT-säkerhet

Iakttagelser

Av intervju med datachefen framgår att kommunen genomför kontinuerliga hälso-check av IT-miljön.

Detta innebär bl.a. kontroll av nätverksinfrastrukturen följt av en detaljerad granskning av kommunens brandväggar. Granskningen är dokumenterad och har genomförts under januari 2017.

Ytterligare hälso- och säkerhetschecker har genomförts under april 2017, dock saknas dokumentation kopplad till kontrollen.

Under juli 2017 har en större GAP-analys med sikte på informationssäkerhet genomförts. Vi har tagit del av dokumentationen.

Kontroll och hälsocheck av behörighetssystem har genomförts under augusti 2017, dock saknas dokumentation.

Samtliga kontroller har genomförts av externa utförare i syfte att säkerställa en objektivitet i bedömningarna.

Kommentarer

Resultaten av GAP-analysen påvisar en del centrala förbättringsområden. Nedan redogörs för ett urval av dessa områden:

- behovet av spridning av befintligt ramverk i kommunen avseende informationssäkerhet.
- verksamheterna har kommit olika långt i informationssäkerhetsarbetet.
- olika rutinerna inom förvaltningarna vid avslutad eller förändrad anställning.
- metoder och verktyg för utbildningsinsatser är olika implementerade i organisationen.
- styrande dokument finns på plats men det finns delar som inte är färdigimplementerade.
- styrning av behörigheter.
- hanteringen av sekretessavtal med externa leverantörer hanteras olika inom förvaltningarna.
- utveckling av regelverk och lösningar inom kontinuitetsplanering.
- uppföljning och efterlevnad av styrdokument.

Kommentarer

Vi anser att samtliga kontroller och hälsochecker ska dokumenteras.

Vi bedömer initiativet till en GAP-analys som positiv som på ett tydligt sätt redogör för utvecklingsområden samt befintliga brister. Ett viktigt steg i denna process är hanteringen av resultaten av GAP-analysen samt framtagande av en åtgärdsplan. Av intervju med datachefen framgår att förbättringsarbetet kommer att presenteras för kommunstyrelsen under våren 2018.

12 Sammanfattande bedömning och rekommendationer

Sammanfattningsvis kan konstateras att det finns tydlig organisation avseende IT-verksamheten. Det finns en medvetenhet kring befintliga brister, där ett förbättrings-arbete har påbörjats.

Utifrån våra iakttagelser bedömer vi att följande punkter bör ses över:

- Kommunstyrelsen bör inom ramen för sin uppsiksplikt samt i egenskap av ansvarig nämnd för kommunens IT-verksamhet genomföra en uppföljning av huruvida nämnderna/styrelserna efterlever gällande styrdokument.
- Kommunstyrelsen bör tillse att de nämnder/styrelser som ligger efter i implementeringsarbetet arbetar fram en åtgärds-/handlingsplan.
- Kommunstyrelsen bör sträva efter en homogen nivå inom nämnder och styrelser vad gäller kunskap och medvetandegrad gällande informationssäkerhet.
- En genomgång av styrdokumenten bör genomföras, där styrdokumentens aktualitet bör framgå av dokumentens framsida. Likaså bör möjligheterna till att reducera antalet riktlinjer och rutiner sonderas.
- Genomförda kontroller avseende IT-miljön bör alltid dokumenteras. Vad gäller externa utförare bör dokumentationskrav framgå av beställningen.
- Genomförd GAP-analys bör uppmärksammas av samtliga nämnder. Kommunstyrelsen ansvarar för uppföljning av analysen samt att framkomna brister åtgärdas.

I samband med faktagranskningen har det framkommit att ett förbättringsarbete har påbörjats inom arbetsgruppen för GDPR med att uppdatera samtliga rutiner, regler, riktlinjer och blanketter med ambitionen att vara klara till den 25 maj 2018.

Viktoria Bernstam

Revisor

Kristian Gunnarsson

Kundansvarig