IT-styrning

Nordanstigs kommun

Juni 2021

Robert Bergman, Cert. kommunal revisor, Projektledare

Markus Månsson, Projektmedarbetare

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Nordanstig kommun granskat kommunens IT-styrning. Syftet med granskningen har varit att bedöma om IT-styrningen i kommunen är ändamålsenlig och om detta sker med tillräcklig intern kontroll. Revisionsobjektet i granskningen har varit kommunstyrelsen.

Utifrån genomförd granskning är vår samlade bedömning att IT-styrningen i kommunen inte helt är ändamålsenlig. Den interna kontrollen bedöms ej vara tillräcklig.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten.

Revisionsfrågor	**Bedömning**
Finns en dokumenterad och kommunicerad struktur och modell för IT-styrning?	Delvis 
Finns ändamålsenliga styrande dokument för IT?	Delvis 
Innehåller de styrande dokumenten relevanta delar?	Delvis 
Uppföljning och utvärdering av upprättad styrning	Nej 

Rekommendationer

I syfte att utveckla verksamheten lämnas följande rekommendationer till kommunstyrelsen:

- Upprätta och etablera en IT-policy där de övergripande styrande principerna hur kommunens IT ska styras finns reglerade.
- Tydliggöra och dokumentera kommunstyrelsens roll och ansvar avseende styrningen av kommunens IT.
- Kommunstyrelsen bör säkerställa att styrande dokument för viktiga IT-relaterade processer upprättas, exempelvis hur IT-projekt ska genomföras och hur behörigheter ska hanteras.
- Säkerställa att upprättad styrning följs och och utvärderas på ett regelbundet sätt för att säkerställa efterlevnad.

Innehållsförteckning

Sammanfattning	1
Inledning	3
Bakgrund	3
Syfte och revisionsfrågor	3
Revisionskriterier	3
Avgränsning	3
Metod	3
Granskningsresultat	5
Revisionsfråga 1 - Struktur och modell för IT-styrning	5
Iakttagelser	5
Bedömning	5
Revisionsfråga 2 - Styrande dokument för styrning av IT	6
Iakttagelser	6
Bedömning	6
Revisionsfråga 3 - Styrdokumentens omfattning	7
Iakttagelser	7
Bedömning	7
Revisionsfråga 4 - Uppföljning och utvärdering av upprättad styrning	7
Iakttagelser	7
Bedömning	8
Samlad bedömning	9
Rekommendationer	9
Sammanfattande bedömningar utifrån revisionsfrågor	10

Inledning

Bakgrund

IT-styrning är konsten att styra en verksamhet så att IT tillför så stort värde som möjligt för verksamheten. Detta innebär bland annat att skapa en organisations- och leveransmodell som stödjer verksamhetens övergripande mål, att definiera processer för hantering av IT-frågor på kort och lång sikt samt att kontinuerligt följa upp att IT-organisationen levererar i tid med rätt kvalitet och till rätt kostnad.

Processer och kunskaper behövs för att hantera IT-ledningsfrågor, strategisk IT-utveckling eller att hantera verksamhetsplanen i en organisation. En bristfällig IT-styrning riskerar att försämra verksamhetens effektivitet samt vara kostnadsineffektiv, tidskrävande och säkerhetsmässigt undermålig. Utan en god IT-styrning finns risk för en ineffektiv relation med verksamheten.

Revisorerna har i sin riskanalys för 2021 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att IT-verksamheten bedrivs på ett för kommunen ändamålsenligt sätt och har därför gett PwC i uppdrag att granska IT-styrningen.

Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om kommunstyrelsen säkerställer att IT-styrningen i kommunen är ändamålsenlig och sker med tillräcklig intern kontroll.

Granskningen avser att besvara nedanstående revisionsfrågor:

- Finns en dokumenterad och kommunicerad struktur och modell för IT-styrning?
  - Fokus på tydlig organisation, med etablerade roller och ansvarsfördelning som hanterar styrning och ledning av kommunens IT.
- Finns ändamålsenliga styrande dokument för IT?
  - Fokus på förekomst av styrning i form av IT-strategi, handlingsplan, samt IT-policy med tillämpliga riktlinjer och instruktioner för nyttjande av IT.
- Innehåller de styrande dokumenten relevanta delar?
  - Fokus om den tar hänsyn till samtliga delar av IT-verksamheten, dvs system, infrastruktur, processer, projekt, förvaltning och styrande principer för de olika delarna som IT-verksamheten omfattar.
- Uppföljning och utvärdering av upprättad styrning
  - Fokus på efterlevnad av styrande dokument samt rapportering till kommunstyrelsen.

Revisionskriterier

- Kommunallagen
- Relevanta styrdokument avseende styrning och ledning av IT

Avgränsning

I tid avgränsas granskningen till år 2021 samt till granskningens revisionsfrågor.

Metod

Granskningen genomförs enligt PwC:s metodik för IT mognadsanalys (ITM):

- Genomgång av tillgänglig dokumentation, däribland policys och riktlinjer.
- Intervjuer/avstämningar med kommunens Digitaliseringsstrateg, Kommunchef samt Kommunstyrelsens ordförande.

Rapporten har faktakontrollerats av intervjuade företrädare för kommunen.

Granskningsresultat

Revisionsfråga 1 - Struktur och modell för IT-styrning

Iakttagelser

I dokumentet Riktlinjer för IT-förvaltning definieras organisation och roller för förvaltning av kommunens IT- och digitala system. Exempelvis definieras följande roller och ansvar:

- Objektägare och objektägare IT
- Förvaltningsledare och förvaltningsledare IT
- Objektspecialist
- IT-specialist
- Förvaltningsarkitekturstyrgrupp
- Förvaltningsobjektstyrgrupp
- Förvaltningsledningsgrupp
- Förvaltningsledningsnätverk

Under intervju beskrivs att det IT-relaterade arbetet till stor del leds och styrs av kommunens Digitaliseringsstrateg. Det framgår dock att Digitaliseringsstrategens uppdrag och ansvar inte är dokumenterat.

I granskningen framkommer att kommunstyrelsens ansvar gällande IT-styrning inte är dokumenterad (exempelvis i en IT-policy). Däremot beskrivs kommunstyrelsens ansvar avseende informationssäkerhet i informationssäkerhetspolicyn. I informationssäkerhetspolicyn anges även ansvaret avseende informationssäkerhet för andra roller i organisationen (exempelvis informationssäkerhetsansvarig och informationsägare).

I granskningen kan det inte styrkas att det finns en dokumenterad och kommunicerad ansvarsfördelning för inköp och upphandling av IT-stöd.

Bedömning

Finns en dokumenterad och kommunicerad struktur och modell för IT-styrning? Fokus på tydlig organisation, med etablerade roller och ansvarsfördelning som hanterar styrning och ledning av kommunens IT.

Vår bedömning är att revisionsfrågan är delvis uppfylld. Bedömningen baseras på följande:

- Organisation och roller för förvaltning av kommunens IT- och digitala system har definierats i styrande dokument.
- Informationssäkerhetspolicyn anger roller och ansvar avseende informationssäkerhet i kommunen.

- Kommunstyrelsens ansvar gällande IT-styrning är inte dokumenterad, exempelvis i en IT-policy.
- Det kan inte styrkas att det finns en dokumenterad och kommunicerad ansvarsfördelning för inköp och upphandling av IT-stöd.

Revisionsfråga 2 - Styrande dokument för styrning av IT

Iakttagelser

I granskningen framgår att följande styrdokument relaterat till IT finns fastställda:

Dokument	Fastställd av	Kommentar
Riktlinjer för IT-förvaltning	Kommunens ledningsgrupp	Giltig till och med 2023-12-31
Riktlinjer för lagring av digital information	Kommunens ledningsgrupp	Giltig till och med 2021-12-31
Riktlinjer för e-post	Kommunstyrelsen	Giltig till och med 2020-05-24
Informationssäkerhets -policy	Kommunfullmäktige	Giltig till och med 2023-12-31
Riktlinje för informationssäkerhet	Kommunstyrelsen	Giltig till och med 2023-12-31

Under intervju framgår att kommunen saknar en etablerad och fastställd IT-policy. Det framgår även att det saknas en aktuell och beslutad IT-strategi. Det finns dock ett pågående arbete med att etablera en ny IT-strategi.

I riktlinjen för informationssäkerhet anges att det ska finnas kontinuitetsplaner upprättade för kritiska verksamhetsprocesser. Under intervju framgår dock att det saknas upprättade kontinuitetsplaner för flera av kommunens kritiska IT-lösningar.

Bedömning

Finns ändamålsenliga styrande dokument för IT? Fokus på förekomst av styrning i form av IT-strategi, handlingsplan, samt IT-policy med tillämpliga riktlinjer och instruktioner för nyttjande av IT.

Vår bedömning är att revisionsfrågan är delvis uppfylld. Bedömningen baseras på följande:

- Det finns etablerade riktlinjer relaterat till IT-förvaltning, lagring av digital information samt för användning av e-post. I sammanhanget noteras att giltigheten för dokumentet Riktlinjer för e-post har löpt ut.
- Informationssäkerhetspolicy och riktlinje för informationssäkerhet finns antagna.
- Det saknas en IT-policy som anger styrande principer för kommunens IT-verksamhet. Det saknas även en aktuell IT-strategi.

Revisionsfråga 3 - Styrdokumentens omfattning

Iakttagelser

I kommunens Riktlinjer för IT-förvaltning anges styrande principer för förvaltning av kommunens infrastruktur och IT-lösningar. Riktlinjen beskriver kommunens modell för systemförvaltning samt roller och ansvar. I riktlinjen beskrivs även vad de olika förvaltningsplanerna ska innehålla, vilket är de operativa styrdokumenten som anger vad som ska göras under året avseende förvaltning av kommunens IT. Övergripande styrprinciper för drift finns angivet i riktlinjen för informationssäkerhet.

Nordanstigs kommuns IT driftas till stor del av det kommunala bolaget Fiberstaden AB, som ägs tillsammans med Hudiksvalls kommun. Granskningen visar att det saknas dokumenterade avtal/överenskommelser gällande servicenivåer, s k SLA[1]. Av intervjuer framgår att det finns behov av att reglera förhållandet mellan kommunen och Fiberstaden, men att detta inte har skett.

I riktlinjen för informationssäkerhet anges övergripande styrprinciper för behörighetshantering. Det framkommer dock under intervju att det saknas dokumenterade riktlinjer/rutiner för behörighetshantering samt förändringshantering och licenshantering. Vidare beskrivs det under intervju att det saknas en etablerad och antagen projektmodell för genomförande av IT-relaterade projekt. Det anges dock att det finns ett pågående arbete med att utvärdera och eventuellt implementera en projektmodell inom kommunen.

Bedömning

Innehåller de styrande dokumenten relevanta delar? Fokus om den tar hänsyn till samtliga delar av IT-verksamheten, dvs system, infrastruktur, processer, projekt, förvaltning och styrande principer för de olika delarna som IT-verksamheten omfattar.

Vår bedömning är att revisionsfrågan är delvis uppfylld. Bedömningen baseras på följande:

- Det finns styrande dokument avseende förvaltning av kommunens infrastruktur och IT-lösningar.
- Det saknas styrande dokument för viktiga IT-processer såsom behörighetshantering, förändringshantering och licenshantering. Det saknas även en etablerad och antagen projektmodell för genomförande av IT-relaterade projekt.

Revisionsfråga 4 - Uppföljning och utvärdering av upprättad styrning

Iakttagelser

Granskningen har inte kunnat styrka att det skett någon uppföljning eller utvärdering hur upprättade styrdokument efterlevs. Det framkommer under intervju att efterlevnaden av kommunens policys och riktlinjer relaterat till IT och informationssäkerhet (se tabell i revisionsfråga 1) inte följs upp.

Granskningen visar att kommunstyrelsen 2021-04-07 har fått information om kommunens IT- och digitaliseringsarbete. Av protokollet framgår att kommunstyrelsen

[1] Service level agreement - avtal/kontrakt som definierar vad en kund kan förvänta sig för servicenivåer från leverantören.

bland annat informerades om vision och mål för IT- och digitaliseringsarbetet, olika former av samverkan samt prioriterade områden.

På tjänstemannanivå följs kommunens IT-relaterade mål upp på årlig basis av kommunens Digitaliseringsstrateg och rapporteras till kommunens ledningsgrupp. Utöver detta har även Digitaliseringsstrategen regelbundna möten med kommunchefen avseende det IT-relaterade arbetet.

Bedömning

Uppföljning och utvärdering av upprättad styrning. Fokus på efterlevnad av styrande dokument samt rapportering till kommunstyrelsen.

Vår bedömning är att revisionsfrågan inte är uppfylld. Bedömningen baseras på följande:

- Det sker ingen uppföljning av efterlevnad avseende kommunens policys och riktlinjer som relaterar till IT.
- Rapportering avseende det IT-relaterade arbetet görs av kommunchefen till Kommunstyrelsen på årlig basis.

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Nordanstig kommun granskat kommunens IT-styrning. Syftet med granskningen har varit att bedöma om IT-styrningen i kommunen är ändamålsenlig och om detta sker med tillräcklig intern kontroll. Revisionsobjektet i granskningen har varit kommunstyrelsen.

Utifrån genomförd granskning är vår samlade bedömning att IT-styrningen i kommunen inte helt är ändamålsenlig. Den interna kontrollen bedöms ej vara tillräcklig.

Rekommendationer

I syfte att utveckla verksamheten lämnas följande rekommendationer till kommunstyrelsen:

- Upprätta och etablera en IT-policy där de övergripande styrande principerna hur kommunens IT ska styras finns reglerade.
- Tydliggöra och dokumentera kommunstyrelsens roll och ansvar avseende styrningen av kommunens IT.
- Kommunstyrelsen bör säkerställa att styrande dokument för viktiga IT-relaterade processer upprättas, exempelvis hur IT-projekt ska genomföras och hur behörigheter ska hanteras.
- Säkerställa att upprättad styrning följs och och utvärderas på ett regelbundet sätt för att säkerställa efterlevnad.

Sammanfattande bedömningar utifrån revisionsfrågor

Revisionsfråga	Bedömning	
Finns en dokumenterad och kommunicerad struktur och modell för IT-styrning?	**Delvis** Organisation och roller för förvaltning av kommunens IT- och digitala system har definierats i styrande dokument. Informationssäkerhetspolicyn anger roller och ansvar avseende informationssäkerhet i kommunen. Kommunstyrelsens ansvar gällande IT-styrning är inte dokumenterad, exempelvis i en IT-policy. Det kan inte styrkas att det finns en dokumenterad och kommunicerad ansvarsfördelning för inköp och upphandling av IT-stöd.	
Finns ändamålsenliga styrande dokument för IT?	**Delvis** Det finns etablerade riktlinjer relaterat till IT-förvaltning, lagring av digital information samt för användning av e-post. I sammanhanget noteras att giltigheten för dokumentet Riktlinjer för e-post har löpt ut. Informationssäkerhetspolicy och riktlinje för informationssäkerhet finns antagna. Det saknas en IT-policy som anger styrande principer för kommunens IT-verksamhet. Det saknas även en aktuell IT-strategi.	
Innehåller de styrande dokumenten relevanta delar?	**Delvis** Det finns styrande dokument avseende förvaltning av kommunens infrastruktur och IT-lösningar. Det saknas styrande dokument för viktiga IT-processer såsom behörighetshantering, förändringshantering och licenshantering. Det saknas även en etablerad och antagen projektmodell för genomförande av IT-relaterade projekt.	

Uppföljning och utvärdering av upprättad styrning	**Nej** Det sker ingen uppföljning av efterlevnad avseende kommunens policys och riktlinjer som relaterar till IT. Rapportering avseende det IT-relaterade arbetet görs av kommunchefen till Kommunstyrelsen på årlig basis.

2021-06-22

Hanna Franck Larsson

Uppdragsledare

Robert Bergman

Projektledare

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Nordanstigs kommun enligt de villkor och under de förutsättningar som framgår av projektplan från den 2021-04-16. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.