Granskningsrapport 2022
Genomförd på uppdrag av revisorerna

Granskning av kommunstyrelsens uppsikt och styrning av IT- och informationssäkerhet

Nässjö kommun

Building a better working world

Innehåll

1. Sammanfattning

EY har genomfört en granskning på uppdrag av de förtroendevalda revisorerna i Nässjö kommun. Granskningen har syftat till att bedöma om kommunstyrelsen har en tillräcklig uppsikt och kontroll avseende IT- och informationssäkerheten.

Nässjö kommun är medlem i Höglandsförbundet. Ett av förbundets verksamhetsområden utgörs av Höglandets IT. Höglandets IT är höglandskommunernas gemensamma IT-avdelning och levererar IT-infrastruktur till kommunerna.

Vår sammanfattande bedömning är att kommunstyrelsen delvis har en tillräcklig uppsikt och kontroll avseende IT- och informationssäkerheten.

Vi bedömer att det finns en tydlig ansvarsfördelning för hur IT- och informationssäkerhetsarbetet ska bedrivas. Ansvarsfördelningen framgår av samverkansavtal med Höglandsförbundet samt kommunens policyer. Vi bedömer dock att kommunen kan tydliggöra hur incidenter avseende informationssäkerhet ska hanteras i den egna organisationen.

Vidare bedömer vi att kommunstyrelsen inte i tillräcklig utsträckning har uppsikt över verksamheten som bedrivs i Höglandets IT samt de frågor som kan inverka på kommunens utveckling. Granskningen visar att kommunstyrelsen inte har definierat vad uppsiktsplikten innebär samt att det inte finns någon definierad strategi kopplat till kommunstyrelsens uppsiktsplikt gentemot kommunalförbundet.

Vi noterar att delar av kommunstyrelsen har tillgång till information via förbundets utskott och direktion. Samtidigt gäller ansvaret för uppsiktsplikten hela kommunstyrelsen. Det är därför viktigt att information från tillfällen där endast delar av styrelsen deltar återrapporteras till hela styrelsen.

Kommunstyrelsen rekommenderas att:

- Tydliggöra ansvar, process och uppföljning av incidentrapportering.
- Definiera vad uppsiktsplikten gentemot kommunalförbundet innebär samt hur den ska utövas.
- Utöka uppföljningen till att omfatta specifika iakttagelser om hur Höglandets IT bedriver sitt arbete gentemot Nässjö kommun.

2. Inledning

2.1. Bakgrund

Enligt reglementet är det kommunstyrelsens ansvar att tillvarata kommunens intressen och ha uppsikt över kommunal verksamhet som bedrivs i sådana kommunalförbund som kommunen är medlem i. Kommunstyrelsen har i uppdrag att utforma och utarbeta riktlinjer och ramar för styrningen av hela den kommunala verksamheten. Därtill ansvarar kommunstyrelsen för de kommunövergripande IT-systemen samt utvecklingen av organisationens digitalisering samt IT och kommunikation.

Nässjö kommun, både nämnder och förvaltningar, hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs det att styrning och löpande arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig samt har tillräckligt starkt skydd.

Det är av vikt att samverkan med förbundet sker effektivt. Likaså att det inom kommunen finns en god uppsikt över förbundets verksamheter.

Kommunrevisionen har med bakgrund av sin risk- och väsentlighetsanalys beslutat att granska huruvida kommunstyrelsen har en tillräcklig kontroll och uppsikt avseende IT- och informationssäkerheten.

2.2. Syfte och revisionsfrågor

Granskningen har syftat till att bedöma om kommunstyrelsen har en tillräcklig uppsikt och kontroll avseende IT- och informationssäkerheten.

I granskningen besvaras följande revisionsfrågor:

- Finns det en tydlig organisering inom kommunen för IT-och informationssäkerhetsfrågor, samt vilka organisatoriska samordningsformer finns mellan förbundet och kommunen på området?
- Finns det en tydlig ansvarsfördelning och tillräcklig samordning med Höglandsförbundet avseende incidenthantering?
- Är återrapporteringen till kommunstyrelsen och sedermera kommunens rapportering av IT- och informationssäkerhetsarbetet tillräcklig?
- Vilka har behörighet att publicera information på kommunens hemsida?
    - Finns det någon dokumenterad rutin som säkerställer att inte obehöriga har tillgång till systemet?

2.3. Genomförande och avgränsning

Granskningen grundas på dokumentstudier och intervjuer med tjänstepersoner inom kommunstyrelsens förvaltning och Höglandets IT samt Höglandsförbundet. Intervjuer har även genomförts med kommunstyrelsens presidium. Se källförteckning för mer ingående beskrivning.

Granskningen är avgränsad till att omfatta kommunstyrelsens styrning och uppsikt över IT-och informationssäkerhetsarbetet.

2.4. Revisionskriterier

Granskningens bedömningar utgår från följande revisionskriterier:

- Kommunallagen
- Kommunstyrelsens reglemente

Revisionskriterierna beskrivs mer ingående i avsnitt 3.

3. Granskningsresultat

3.1. Revisionskriterium

Kommunallagen 6 kap

Styrelsen ska leda och samordna förvaltningen av kommunens angelägenheter. Styrelsen ska även ha uppsikt över verksamhet som bedrivs i kommunalförbund.

Vidare ska styrelsen följa de frågor som kan inverka på kommunens eller regionens utveckling och ekonomiska ställning.

3.2. Iakttagelser

3.2.1. Ansvarsfördelning

Höglandsförbundet och kommunens ansvar för IT- och informationssäkerhetsarbetet finns reglerat i styrande dokument. 2019 tecknades ett samverkansavtal mellan höglandskommunerna och Höglandets IT (HIT). Avtalet syftar till att konkretisera förbundsordningens innehåll. I avtalet framgår höglandskommunernas och HIT:s åtagande. Enligt avtalet ansvarar HIT bland annat för att leverera IT-drift och support. I samverkansavtalet framgår att HIT ansvarar för incidentrapportering. Avtalet fastställer att incidenterna ska rapporteras på nästkommande ledningsgruppsmöte.

Fullmäktige har antagit en IT-säkerhetspolicy och en informationssäkerhetspolicy. Båda policyerna är förbundsgemensamma och därmed antagna av samtliga kommuner i förbundet [1].

Policyerna beskriver roller och ansvar för olika funktioner inom förbundet och kommunen vad gäller arbetet med informationssäkerhet och IT-säkerhet. Policyn för IT-säkerhet omfattar hur verksamhetens IT-relaterade tillgångar ska kunna skyddas, exempelvis maskinvaror och programvaror. Målsättningen är att säkerställa en robust och säker drift av systemen. Informationssäkerhetspolicyn utgår från att skapa och upprätthålla rutiner och skydd av information utifrån fyra aspekter:

- Konfidentialitet: att information inte tillgängliggörs eller avslöjas till obehörig
- Riktighet: att information är korrekt, aktuell och fullständig
- Tillgänglighet: att information är åtkomlig och användbar av behörig
- Spårbarhet: att händelser i informationsbehandlingen ska kunna spåras

[1] 2020-03-23 och 2020-01-30

Tillskillnad mot IT-säkerhetspolicyn är informationssäkerhetspolicyn inte begränsad till säkerhet i system utan omfattar även information som uttrycks muntligen eller i skrift.

Enligt informationssäkerhetspolicyn ansvarar kommunstyrelsen för att samordna informationssäkerhetsarbetet genom att årligen fastställa en övergripande handlingsplan. Kommunstyrelsen har antagit en handlingsplan för informationssäkerhetsarbetet[2]. I informationssäkerhetspolicyn framgår vidare att varje nämnd och bolagsstyrelse ansvarar för informationssäkerheten inom sitt verksamhetsområde. Styrelse och nämnder ansvarar därmed för att medarbetarna har tillräcklig kunskap om informationssäkerhet samt att det finns en tillförlitlig hantering av informationen. HIT ansvarar i sin tur för att den tekniska miljön är säker.

Sedan 2020 har kommunens informationssäkerhetssamordnare rollen som dataskyddssamordnare. I samordnarens roll ligger att samordna kommunens informationssäkerhetsarbete. Samordnaren har anordnat utbildningar för kommunens chefer samt tagit fram ovan nämnd handlingsplan för informationssäkerhet. Höglandsförbundet har en informationssäkerhetsspecialist som stöttar kommunerna i arbetet.

Vid intervju med representanter från kommunen och HIT framförs att det är tydligt hur ansvaret för den dagliga driften är fördelat. Parterna har däremot identifierat ett behov av att tydliggöra ansvarsfördelningen i utvecklingsfrågor som exempelvis digitalisering.

3.2.2. Samordningsformer

Samverkansansavtalet innehåller en beskrivning över olika samordningsformer. Samverkan bedrivs inom strategigrupp, ledningsgrupp och nätverksgrupper. Avtalet fastställer vilka som ingår i samordningsformerna samt målsättningar, mötesplan och vem som är sammankallande för respektive samverkansform.

I samordningsformerna finns representanter i form av bl.a. kommundirektörer, förvaltningschefer och digitaliseringsstrateger. Se avsnitt 7 för en illustration av samordningsformerna.

I erhållna presentationer från nätverksträffar framgår att nätverken bland annat har kartlagt vilka insatser som har genomförts och verksamheternas framtida behov.

3.2.3. Incidenthantering

Samverkansavtalet innehåller ett avsnitt avseende incidentrapportering. Incident definieras enligt avtalet som ett oplanerat avbrott i en IT-tjänst eller reduktion av kvaliteten hos en IT-tjänst. I avsnittet om incidentrapportering framgår att:

[2] 2021-08-18

"Varje kritisk incident som inträffar ska avrapporteras på nästkommande ledningsgruppsmöte efter aktuell incident. HIT är ansvarig för incidentrapporteringen."

För att bedöma om en incident räknas som kritisk finns en process som utgår från allvarlighetsgrad, angelägenhet och påverkan. Ledningsgruppen består av digitaliseringsstrateger från kommunerna samt HIT ledningsgrupp.

Kommunens informationssäkerhetspolicy och it-säkerhetspolicy beskriver inte vilken funktion som ansvarar för att rapportera incidenter eller hur de ska rapporteras. Vid intervju framförs att medarbetare i kommunen ska anmäla incidenter till HIT IT-support.

Vid incidenter kopplat till personuppgifter eller informationssäkerhet utreds incidenten av Höglandsförbundets informationssäkerhetsspecialist och dataskyddsombud, och i samverkan med HIT IT-säkerhetsgrupp om det är IT-relaterat. Höglandsförbundet har tagit fram ett informationsmaterial om informationssäkerhet för anställda och förtroendevalda. Materialet finns publicerat på kommunens intranät. Det framgår att incidenter omedelbart ska anmälas till HIT support och närmsta chef.

3.2.4. Behörighet till kommunens hemsida

Kommunikationschefen är systemansvarig för kommunens hemsida (SiteVision). Kommunikationsenheten har en dokumenterad rutin för behörighetshantering till kommunens hemsida. Rutinen omfattar hur behörigheter ska tilldelas, förändras och tas bort. Det framgår vem som är ansvarig för respektive moment. Enligt rutinen får behörigheter endast beställas av ansvarig chef.

Vid priviligierad behörighet är det däremot systemägare som har mandat att tilldela, förändra eller ta bort behörigheten. Privilegierad behörighet innebär en utökad behörighet där personen exempelvis kan skapa nya användare och tilldela behörighet till andra. Det finns två tjänstepersoner i kommunen med priviligierad behörighet till kommunens hemsida[3].

Vid intervju framförs att kommunen är restriktiva med vilka som ska ha möjlighet att publicera information på hemsidan. Kommunikationschefen och kommunikatörer har bred publiceringsrätt och kan därmed publicera information på hemsidans samtliga sidor. I övrigt är behörigheterna begränsade till 25 redaktörer som enbart kan publicera information på de sidor som berör den egna verksamheten.

Enligt rutinen för behörighetstilldelning ansvarar systemansvarig för att göra löpande kontroller för att ta bort eventuella användare som inte ska ha kvar behörigheten. Kontrollerna genomförs enligt uppgift två gånger om året samt i samband med att nya redaktörer registreras.

[3] Kommunikationschef och webbutvecklare.

3.2.5. Uppföljning och återrapportering

Det finns inga riktlinjer för hur kommunstyrelsens uppsiktsplikt ska utövas. Kommunstyrelsen följer upp HIT verksamhet genom att ta del av Höglandsförbundets delårsrapport och årsredovisning. Delårsrapporten och årsredovisningen innehåller ett avsnitt om övergripande verksamhetsinformation, måluppfyllelse och förväntad utveckling för HIT. Rapporterna innehåller ingen specifik information avseende IT-säkerheten i kommunen.

Höglandsförbundets förbundsdirektör och ekonomichef deltar årligen vid ett kommunstyrelsesammanträde för dialog i samband med att budgeten ska fastställas. Enligt uppgift har HIT deltagit under kommunstyrelsens sammanträden på förekommen anledning i samband med att styrelsen skulle anta styrande dokument på området. Höglandsförbundets informationssäkerhetssamordnare deltog i samband med att kommunstyrelsen antog IT-säkerhetspolicyn.

Enskilda incidenter följs upp i Höglandsförbundets ledningsgrupp. HIT publicerar incidentrapporter på Höglandsnätet. Höglandsnätet är ett intranät som samtliga medlemskommuner har tillgång till. I incidentrapporterna framgår bland annat när incidenten inträffade, vilken verksamhet och kommun som drabbades, hur den upptäcktes och vilka åtgärder som har vidtagits.

Det sker ingen rapportering av incidenter till kommunstyrelsen. Vidare sker det ingen uppföljning till kommunstyrelsen avseende HIT säkerhetsarbete och riskhantering av system som används i Nässjö kommun.

I samverkansavtalet framgår att avtalet ska följas upp när någon av parterna begär det. Det har inte genomförts någon avtalsuppföljning sedan avtalet tecknades 2019.

Kommunstyrelsens ordförande ingår i Höglandsförbundets arbetsutskott. HIT redovisar tertialrapporter och prognosuppföljningar för utskottet. Kommunstyrelsens ordförande och andre vice ordförande ingår i Höglandsförbundets direktion. Kommunstyrelsens protokoll från 2022 innehåller inget ärende om återrapportering från arbetsutskottet eller direktionen. Kommunstyrelsens ordförande förmedlar viktig information från direktionen i beredningen inför kommunstyrelsens sammanträden.

I kommunstyrelsens protokoll framgår att kommunstyrelsen har tagit del av protokoll från Höglandsförbundets direktions möten under 2022. Direktionens protokoll innehåller ingen kommunspecifik information. Kommunstyrelsens protokoll innehåller inga andra informationsärenden avseende HIT eller IT- och informationssäkerhetsarbetet.

4. Slutsats

Vår sammanfattande bedömning är att kommunstyrelsen delvis har en tillräcklig uppsikt och kontroll avseende IT- och informationssäkerheten.

Vi bedömer att det finns en tydlig ansvarsfördelning för hur IT- och informationssäkerhetsarbetet ska bedrivas. Bedömningen görs mot bakgrund av att ansvarsfördelningen framgår av samverkansavtal samt kommunens policyer. Vi bedömer dock att kommunen kan tydliggöra hur incidenter avseende informationssäkerhet ska hanteras i den egna organisationen.

Vidare bedömer vi att kommunstyrelsen inte i tillräcklig utsträckning har uppsikt över verksamheten som bedrivs i HIT samt de frågor som kan inverka på kommunens utveckling. Granskningen visar att kommunstyrelsen inte har definierat vad uppsiktsplikten innebär samt att det inte finns någon definierad strategi kopplat till kommunstyrelsens uppsiktsplikt gentemot kommunalförbundet. Kommunstyrelsen får övergripande information om HIT arbete via delårsrapport och årsredovisning. Rapporterna innehåller däremot ingen specifik information som rör Nässjö kommun, exempelvis i form av antal incidenter.

Vi noterar att delar av kommunstyrelsen har tillgång till information via förbundets utskott och direktion. Samtidigt gäller ansvaret för uppsiktsplikten hela kommunstyrelsen. Det är därför viktigt att information från tillfällen där endast delar av styrelsen deltar återrapporteras till hela styrelsen.

Revisionsfråga	Svar
▸ Finns det en tydlig organisering inom kommunen för IT-och informationssäkerhetsfrågor, samt vilka organisatoriska samordningsformer finns mellan förbundet och kommunen på området?	Ja. Ansvarsfördelning framgår av samverkansavtal samt kommunens informationssäkerhetpolicy samt IT-säkerhetspolicy. Det finns samverkansformer på både tjänstepersonsnivå samt politisk nivå.
▸ Finns det en tydlig ansvarsfördelning och tillräcklig samordning med Höglandsförbundet avseende incidenthantering?	Delvis. Samverkansavtalet innehåller ett avsnitt om incidenthantering. Kommunens informationssäkerhetspolicy beskriver inte vem som ansvarar för att rapportera incidenter kopplat till informationssäkerhet. Det finns en separat beskrivning av informationssäkerhetsarbetet där det framgår att incidenter ska rapporteras till HIT support.

	Det sker ingen uppföljning över hur många incidenter som har inträffat i kommunen.
▸ Är återrapporteringen till kommunstyrelsen och sedermera kommunens rapportering av IT- och informationssäkerhetsarbetet tillräcklig?	Delvis. Kommunstyrelsen tar del av övergripande information via delårsrapporter och årsredovisning. Rapporterna innehåller ingen specifik information rör Nässjö kommun.
▸ Vilka har behörighet att publicera information på kommunens hemsida? ○ Finns det någon dokumenterad rutin som säkerställer att inte obehöriga har tillgång till systemet?	Information kan publiceras av kommunikationschef, kommunikatörer och redaktörer. Redaktörernas behörighet är begränsad till de sidor som avser den egna verksamheten. Det finns en dokumenterad rutin för hur behörigheter till kommunens hemsida ska hanteras.

Kommunstyrelsen rekommenderas att:

- Tydliggöra ansvar, process och uppföljning av incidentrapportering.
- Definiera vad uppsiktsplikten gentemot kommunalförbundet innebär samt hur den ska utövas.
- Utöka uppföljningen till att omfatta specifika iakttagelser om hur Höglandets IT bedriver sitt arbete gentemot Nässjö kommun.

Carl-Henrik Sölvinger
EY

Anna Färdig
EY

5. Källförteckning

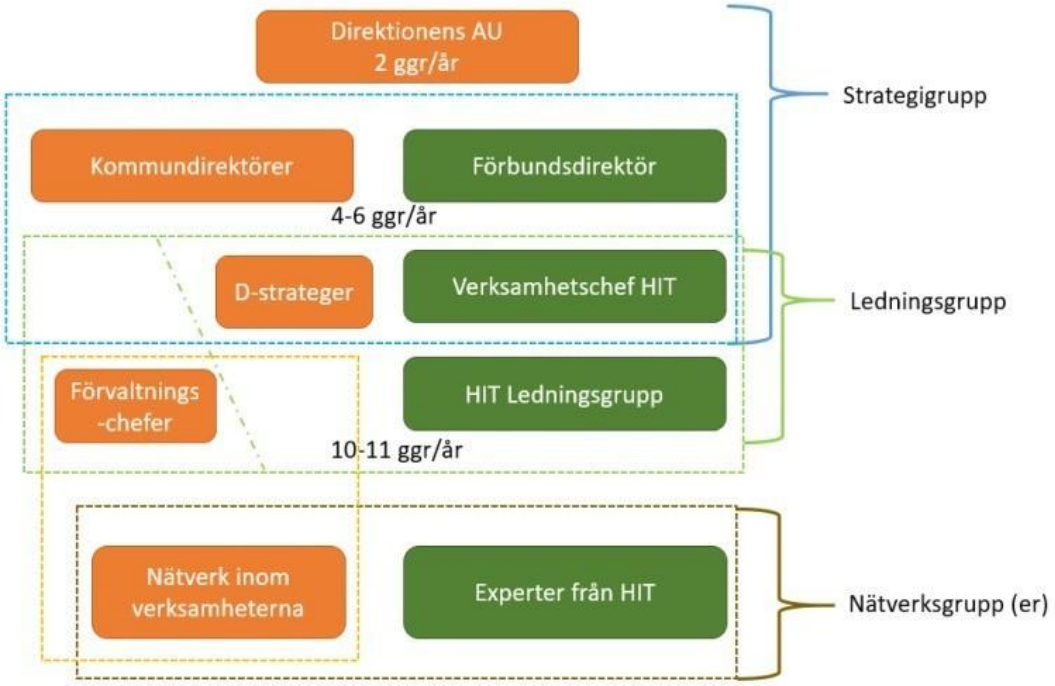
Intervjuade funktioner

- Kommunstyrelsens arbetsutskott
- IT-chef Höglandets IT
- Kommundirektör
- Informationssäkerhets- och dataskyddssamordnare
- Kommunledningsstrateg
- Kommunikationschef
- Dataskyddsombud
- Informationssäkerhetsspecialist
- Enhetschef för IT-säkerhet

Analyserade dokument

- Rutin vid behörighetshantering för kommunens hemsida, 2022-04-06
- Presentation skolnätverk 2022-01-31
- Protokoll kommunstyrelsen 2021–2022
- Samverkansavtal mellan höglandskommunerna och Höglandets IT, 2019
- Intern kontrollplan 2022
- Förbundsordning, höglandsförbundet
- Handlingsplan informationssäkerhet 2021-2022
- IT-säkerhetspolicy
- Informationssäkerhetspolicy
- Informationssäkerhet för anställda och förtroendevalda
- Årsredovisning 2021 Höglandsförbundet

6. Bilaga 1 samordningsformer



Källa: Samverkansavtal 2019. I nätverksgruppen inom HIT ingår även experter från Höglandsförbundet (exempelvis informationssäkerhetsspecialist)