Deloitte.

# Revisionsrapport

## Kommunens IT-organisation

Härjedalens kommun 20 juni 2018

# Innehåll

# Sammanfattning

## Bakgrund och Uppdrag

Kommunens revisorer har beslutat att göra en översiktlig granskning av IT-avdelningen.

## Revisionsfråga

**Revisionsfrågan** är om avdelningens bemanning och organisation är ändamålsenlig utifrån givet uppdrag?

### Sammanfattande bedömning

Vår sammanfattande bedömning är att tydliga rutiner och målstruktur behöver utvecklas för att roller och uppdrag ska vara tydliga för IT-avdelningen. IT-säkerhetsarbetet måste ha högsta prioritet under 2018.

Vi lämnar följande rekommendationer:

- Prioritera IT-säkerhetsarbetet under 2018.
- Utarbeta tydliga rutiner och mål för IT-avdelningen.
- Uppdatera, förenkla och strukturera upp i alla styrdokument som finns och prioritera bland dessa.
- Kartlägg och genomför en risk och sårbarhetsklassning av de ca 50 externa IT-system som finns i kommunen.
- Gör regelbundna formella avrapporteringar till KS omkring incidenter och datasäkerhet.

Östersund 2018-06-20

DELOITTE AB

Kjell Pettersson, Certifierad kommunal revisor, Uppdragsansvarig

# 1 Inledning

## 1.1 Uppdrag och bakgrund

Kommunens revisorer har uppdragit till Deloitte att göra en översiktlig granskning över hur IT-enheten är organiserad och bemannad.

## 1.2 Revisionsfråga och kontrollmål

**Revisionsfrågan** är om avdelningens bemanning och organisation är ändamålsenlig utifrån givet uppdrag?

**Kontrollmål:** Vilka arbetsuppgifter har enheten? Finns det mål för enheten? Hur finansieras verksamheten? Hur arbetar enheten med IT-säkerhet? Finns det någon verksamhetsplan för 2018? Hur följs planen upp? Finns incidentrapportering? Hur rapporteras och följs incidenter upp? Har avdelningen någon extern samarbetspartner (företag, organisation) som har tillgång till avdelningens information?

## 1.3 Revisionskriterier

Underlag för bedömningen är interna regler och riktlinjer.

## 1.4 Avgränsning

Granskningen avser 2018.

## 1.5 Metod

Granskningen genomförs genom dokumentstudier och intervjuer med tjänstemän.

# 2 Resultat

## 2.1 Organisation och bemanning

IT- avdelningen är en stabsenhet som sorterar under kommunledningsförvaltningen, se bilaga 1 organisation och bemanning IT-avdelningen.

IT-avdelningen består av 10 personer och 10 årsarbetare inklusive kansli- och/IT-chef. Totalt antal anställda för hela kansliet och IT-avdelningen är ca 21,5 årsarbetare.

Avdelningen ansvarar för det samordnade IT- stödet till kommunens verksamheter med totalt ca 1300 årsarbetare och ca 850 datorer, ca 800 iPads och 625 mobiltelefoner, mobila bredband som administreras är ca 116 st, 125 elevdatorer och ca 500 laptop för elever samt ca 50 olika adb-system. Även Härjegårdar Fastighets AB ska servas till viss del av IT-avdelningen, enligt avtal.

Enligt IT-chefen är arbetstrycket stort på enheten och det finns lite tid att fokusera på mål/styrdokument, strategier och utvecklingsfrågor.

## 2.2 Styrdokument, uppdrag och övergripande mål

Utgångspunkten för IT-stödet är **kommunfullmäktiges** mål avseende den kommunala servicen det vill säga "servicen ska vara effektiv, flexibel och av hög kvalitet".

**Kommunstyrelsen** är övergripande ansvarig för att leda arbetet och samordna arbetet med säkerhetsfrågor och "ha hand om kommunens PA-system, ekonomisystem, dokument- och ärendesystem, e-postsystem, IT- system, kommunikationssystem, skaderapporteringssystem, passersystem och förtroenderegister (KS reglemente § 3 p 2 och 3).

Kommunledningsutskottet (KLU) är **ledningsgrupp** för arbetet med IT-säkerhet, enligt IT-säkerhetspolicyn. Inga beslut tas i KLU om datasäkerhet.

Enligt Informationssäkerhets Instruktionen från 2009 ska det finnas en IT-ledningsgrupp bestående av IT-chef, kommunalråd, kanslichef, ekonomichef och Informationssäkerhetssamordnare. I praktiken finns det ingen IT-ledningsgrupp utan istället IT-råd för varje förvaltning

utom för samhällsbyggnadsförvaltningen. IT-råden är situations och projektorienterade utifrån aktuellt uppdrag och inträffade händelser. IT-råden består av personer från IT-avdelningen, förvaltningschef samt systemförvaltare.

Respektive nämnd och förvaltning beslutar om behov av förvaltningsspecifika IT-system efter samråd med IT-avdelningen. Systemförvaltare tillika systemansvariga finns utsedda för varje IT-system (ca 50 st).

Följande "styrdokument"har överlämnats från IT-chefen:

**IT-säkerhetspolicy** fastställd av fullmäktige 2005 (KF 83/05). Finns på kommunens hemsida.

**IT-säkerheten i Härjedalens kommun-alla har ett ansvar,** fastställd av KLU 2006-06-14. Innehåller praktiska anvisningar för alla IT-användare, exempelvis att låsa datorn när arbetsrummet lämnas, inte låna ut behörighet och lösenord med mera.

**Informationssäkerhets Instruktion Förvaltning** daterad 2009-10-16 med IT-chef som författare. Dokumentet kallas styrande och handlar om konkretisering av Informationssäkerhetspolicyn från 2005. Bl a framår att IT-ledningsgruppen består av IT-chef, kommunalråd, kanslichef, ekonomichef och informationssäkerhetssamordnare. Ansvarsfördelning på 9 olika nivåer räknas upp, från KS till informationssäkerhetssamordnare. I praktiken tillämpas inte dokumentet och IT-ledningsgruppen finns inte, se 2.2.

**InformationsSäkerhets-Instruktion Användare** från 2016-05-09, med tidigare IT-chef som handläggare. Ett "styrande dokument" för IT-användare i enlighet med Krisberedskapsmyndighetens Basnivå för InformationsSäkerhet (BITS). Innehåller bl a bilagor där användaren ska intyga och skriva under försäkran om personligt ansvar, ansökan om behörighet, godkännande av chef om behörighet, anmälan om avslut av konto i kommunens nätverk i samband med avslutning av anställning, sekretess med mera.

**Telefonpolicy** daterad 2008-02-28 med kansli/IT-avdelningen som författare. Handlar om servicenivå, tillgänglighet och "god telefonkultur".

**Riktlinjer för anskaffning av mobiltelefoner** komplement till informationssäkerhet enligt BITS, med IT-avdelningen som författare daterad 2011-10-03. Översyn pågår av dokumentet.

**Rutin för post och e-post i Härjedalens kommun,** framtaget 2018 och fastställd av kommunchefen juni 2018? ***KLART?***

***Bredbandsstrategi*** finns inte för kommunen utan bygger på regionens - och den nationella strategin och är inte utarbetad särskilt för Härjedalen, enligt uppgift från näringslivsavdelningen och bredbandssamordnaren.

**Riktlinjer för stöldmärkning av kommunens egendom** från 2010-09-09 med IT-avdelningen som avsändare.

**Policy för hantering av datorprogramlicenser** från 2010-09-08 med IT-avdelningen som avsändare där organisation, roller och ansvar behandlas.

### 2.3 Ekonomi IT-avdelningen

Driftbudgeten för 2018 uppgår till ca 5,5 mnkr som till övervägande del är personalkostnader. Budgeterade intäkter är totalt ca 350 kkr från Jämtlands Räddningstjänstförbund, arbetsförmedlingen och Härjegårdar fastighets AB.

Enligt utdrag ur investeringsbudgeten för 2018 finns ca 3,6 mnkr budgeterade för IT-investeringar 2018 varav 2,1 mnkr avser åtgärder för krisledning (MSB). Överförda pågående investeringar från 2017 är ca 1,2 mnkr.

Fullmäktige (§ 66 2018) har beslutat att bevilja 4,5 mnkr ytterligare till IT-investeringar. Exempel på pågående investeringar är inköp av elevdatorer för ca 2,4 mnkr.

Total investeringsbudget för 2018 är ca 7,2 mnkr efter fullmäktigebeslutet, § 66 2018.

### 2.4 Mål och verksamhetsplanering för 2018

I kommunens budget för 2018 framgår följande: "IT-avdelningen arbetar ständigt för att möta de ökade kraven på mobil tillgänglighet och kapacitet som kommer till följd av en allt större mängd användare av datorer, läsplattor och annan utrustning. Samverkan i länet kring e-tjänster är en annan viktig fråga att arbeta med under 2018".

Ingen formell verksamhetsplanering (VP) finns fastställd av Ks för 2018 utan i internt arbetsmaterial för IT-avdelningen framgår det huvudsakliga uppdraget. Uppdraget består bland annat av drift, support, beställning av utrustning, utveckling och säkerhetsarbete. En "aktivitetslista" för pågående och kommande aktiviteter finns upprättat för IT-teknikerna.

I kommunens årsredovisning för 2017 framgår följande om verksamheten: "IT har även under detta år lagt stort fokus på

tillgänglighet, säkerhet och kapacitet där kraven från de olika verksamheterna ständigt ökar. Särskilt fokus på virusskydd och system för back-up av data".

Konkret under 2017 innebar arbetet att tillgodose förvaltningarnas behov av bland annat support, beställningar av nätverks IT- stöd med WIFi och utökade terminaler för IP-telefoni, uppgraderingar av IT-system för e-post med mera. Även ett arbete med att öka IT-driftsäkerheten innefattande bland annat byte av serverhårdvara, uppgradering av serversystem pågår. En "hacker test" dataintrångstest gjordes hösten 2017 av extern utförare för att testa kommunens externt exponerade IP-adresser. Enligt uppgift var resultatet av testet mycket bra.

För närvarande juni 2018 finns ca 100 pågående IT–ärenden i IT-supporten. Supporten består av 3 medarbetare som själva eller med hjälp av IT-teknikerna löser olika problem av varierande omfattning och angelägenhetsgrad. Ca 100 nya ärenden inkommer varje vecka och som rapporteras in i ärendesystemet Duo-station.

### 2.5 Uppföljning och rapportering av bedriven verksamhet

Uppföljning av verksamhet sker internt inom avdelningen genom gruppmöten och arbetsplatsträffar minst 4 gånger varje månad samt vid behov. IT-teknikerna har möten var 14:e dag.

Formella budgetrapporteringar sker i samband med delårsrapport och årsredovisning till KS. Ingen särskild information ges omkring verksamhetsfrågor vid dessa tillfällen. Det är kommunchefen som formellt svarar för budget och eventuell verksamhetsinformation till KS.

Formell incidentrapportering av inträffande oönskade händelser, exempelvis obehörig åtkomst av data eller intrång, virus etc görs rutinmässigt och tas upp **internt** inom IT-avdelningen. Mindre händelser rapporteras i minnes-anteckningar som förs vid IT-avdelningen. Kommunstyrelsen har hittils inte **formellt** informerats om eventuella incidenter.

### 2.6 IT-säkerhet och sekretess

Som framgått i avsnitt 2.1 är arbetstrycket stort på enheten och det finns begränsad tid att fokusera på strategier och utvecklingsfrågor. Däremot anser IT-avdelningen att de har ett väl utvecklat säkerhetsarbete och säkerhetsmedvetande, exempelvis nyligen genomfört intrångstest ("Hack & Pen test"). Dörrkoder och nyckelcylindrar har bytts ut för telerum och serverrum för att öka säkerheten. För 2018 planeras att sätta in kortläsare i serverrum för att uppnå spårbarhet.

Beträffande sekretessbedömning och utlämnande av allmänna handlingar är det IT- och kanslichefen som gör den bedömningen.

Det finns ca 50 olika externa IT-systemleverantörer som vid behov kan ges möjlighet att åtgärda eventuella problem med IT-systemen. Av dessa 50 leverantörer kan alla ges åtkomst via exempelvis VPN-konton till respektive system. Det är alltid IT-avdelningen som "öppnar upp" för externa systemleverantörer.

Risk och sårbarhetsanalyser med säkerhetsklassning saknas och det är när problem uppstår som IT-enheten agerar. Exempel är när kylaggregaten slutade att fungera i serverrummen under vintern 2018 och datordriften låg nere.

Exempel på säkerhetsåtgärder som finns är antivirusskydd (nytt från 2017), skyddsfilter mot virus i e-post och skydd mot okända program som gör att de inte kan laddas ned i datorn.

# 3 Revisionell bedömning

## 3.1 Organisation och bemanning

It-avdelningen behöver arbeta mer förebyggande både strategiskt och utvecklingsmässigt. Genom prioritering från KS i IT-avdelningens verksamhetsplan för 2019 och framåt skapas förutsättningar att detta uppnås med eller utan extern konsulthjälp.

## 3.2 Styrdokument, uppdrag och mål

Som framgår under avsnitt 2.2 finns det många styrdokument och måldokument. Det är svårt att få en bild av hur de hänger ihop och struktur saknas. Många av dokumenten har inte uppdaterats under lång tid och är inte aktuella varken beträffande lagstiftning eller organisation.

IT-säkerhetspolicyn från 2005 är ett exempel på dokument som snarast behöver förnyas och uppdateras.

Tid behöver avsättas för att strukturera i mängden av dokument. En IT-policy med både internt och externt fokus bör bli slutresultatet där endast ett fåtal dokument som verkligen behövs, fastställs av KS.

Det är viktigt att ansvar och befogenheter sammanfaller i de dokument som blir kvar efter genomgången.

Även olika beslutsnivåerna och ansvarsområdena bör tydliggöras mellan kommunstyrelsen, respektive nämnd, KLU, IT-råden och IT-chefen.

## 3.3 Ekonomi

Budget och redovisade kostnader för 2017 överstämmer bra och ett mindre överskott (ca 100 kkr) redovisas för 2017.

Intrycket är att strukturen på budget och redovisning både av kostnader (driften) och utgifter (investeringar) är bra upplagt.

Det är viktigt att MSB-anslaget på 2,1 mnkr inte blandas ihop med övriga verksamheten utan redovisas separat i både budget och redovisning.

### 3.4 Mål, verksamhetsplanering och uppföljning av verksamhet för 2018

Vi saknar en formell verksamhetsplanering för avdelningen som prioriterats och beslutats av KS. I dagsläget finns planeringen som internt arbetsmaterial inom avdelningen, exempelvis "Aktivitetslista".

Tydliga rutiner behöver utarbetas för exempelvis rapportering av oönskade incidenter till KS.

Moment omkring datasäkerhet behöver läggas till i kommunstyrelsens internkontroll plan för 2018.

### 3.5 IT-säkerhet och sekretess

Som framgått i avsnitt 2.1 är arbetstrycket stort på enheten och det har inte funnits tid för att fokusera på strategier och utvecklingsfrågor, vilket innebär att IT-säkerhetsarbetet behöver prioriteras 2018.

Vi vill ändå ge en eloge för att avdelningen genomfört en extern intrångstest "Hack& Pen test". Resultatet av testet borde redovisats för KS, som ytterst är ansvarig.

Om det finns ca 50 olika externa IT-system(en del system med samma leverantör) behöver en risk och sårbarhetsklassning genomföras för att identifiera svagheter eller brister i IT-säkerheten. I dagsläget finns ingen sådan riskanalys.

### 3.6 Sammanfattande bedömning och rekommendationer

Vår sammanfattande bedömning är att tydliga rutiner och målstruktur behöver utvecklas för att roller och uppdrag ska vara tydliga för IT-avdelningen. IT-säkerhetsarbetet måste ha högsta prioritet under 2018.

Vi lämnar följande rekommendationer:

- Prioritera IT-säkerhetsarbetet under 2018.
- Utarbeta tydliga rutiner och mål för IT-enheten.
- Uppdatera, förenkla och strukturera upp i alla styrdokument som finns och prioritera bland dessa.
- Kartlägg och genomför en risk och sårbarhetsklassning av de ca 50 externa IT-system som finns i kommunen.
- Gör regelbundna formella avrapporteringar till KS omkring incidenter och datasäkerhet.

## Intervjuade och uppgiftslämnare

Mats Sjöstedt, IT- och kanslichef

Fredrik Jonasson, ekonom

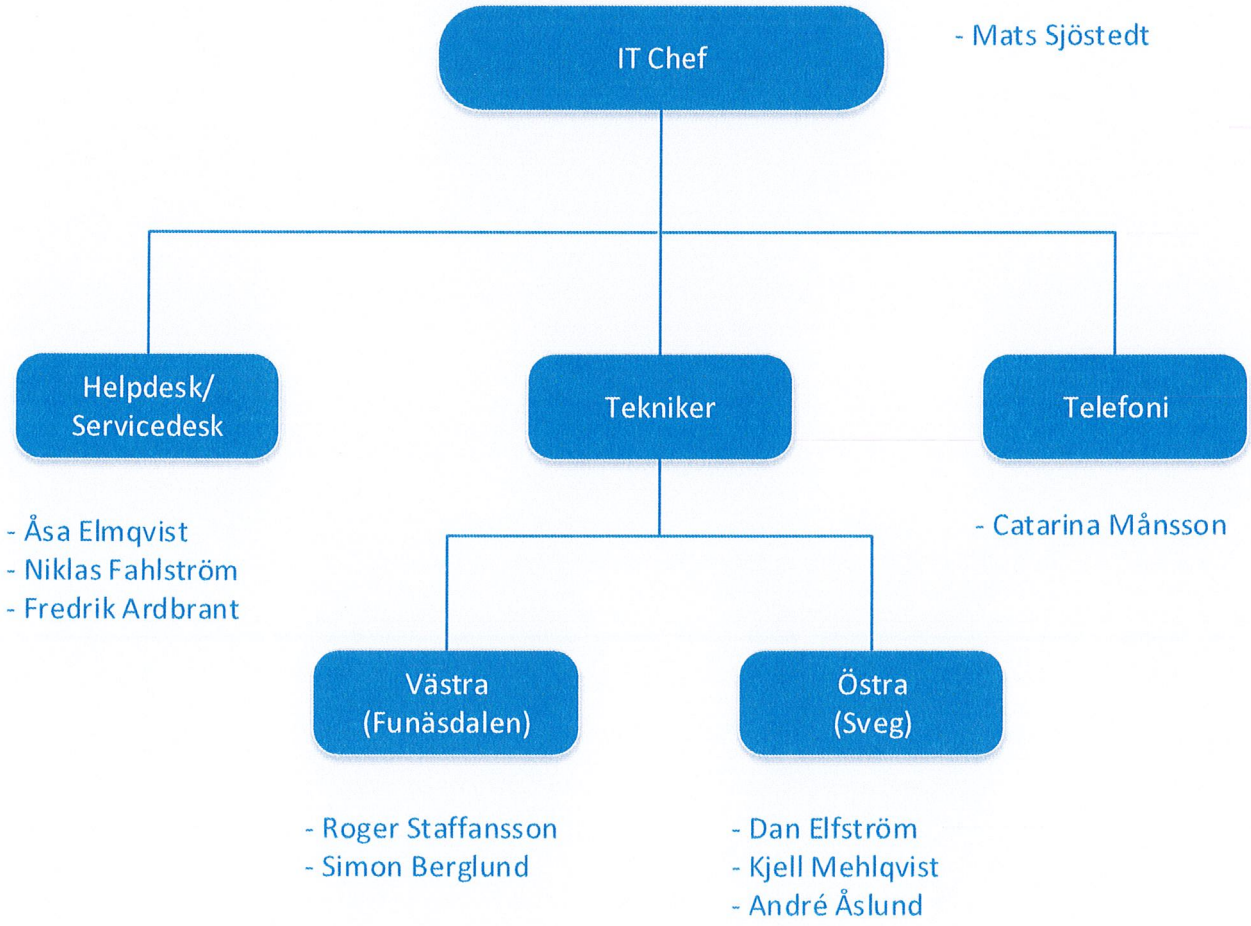
Kjell Mehlqvist, IT-samordnare

Andreé Åslund, IT-samordnare

Åsa Elmqvist, IT-support tekniker

HÄRJEDALENS KOMMUN
HERJEDAELIEN TJIELTE

# Organisation IT




2018-05-24

Deloitte.