Granskning av IT-enheten

Rapport

Malung-Sälens kommun

KPMG AB

2018-10-03

Antal sidor 9

Antal bilagor 3

Malung-Sälens kommun
Granskning av IT-enheten

2018-10-03

Innehållsförteckning

1 Sammanfattning

Vi har av Malung-Sälens kommuns revisorer haft i uppdrag att utföra en granskning av IT-enheten avseende organisation, uppdrag, resursförsörjning samt arbetsformer och rutiner. Syftet med granskningen har varit att bedöma om kommunen har säkerställt en sammanhållen, effektiv, ändamålsenlig och strategisk försörjning och utveckling gällande det verksamhetsstöd som en IT-enhet kan förväntas tillhandahålla. Uppdraget ingår i revisionsplanen för år 2018.

Vi finner att kommunen saknar dokumentation där det framgår vilken roll och ansvar IT-enheten har och framgent ska ha för att bidra till uppfyllandet av kommunens verksamhetsmål. Två övergripande åtgärder planeras för att förändra detta.

Under hösten 2018 ska det påbörjas ett arbete med att ta fram en styrmodell för kommunen. I denna dokumentation ska det, vad vi förstår, även anges vilken roll och ansvar IT-enheten kommer att ha. Parallellt med detta ska de datoriserade verksamhetssystemens information klassas enligt vedertagna metoder. Förvaltningarna ska enligt uppgift vara muntligt informerade om vad som krävs av dem samt vilket stöd som externa konsulter och IT-enheten kommer att bidra med. Arbetet ska vad som uppges leda fram till styrdokument som anger hur ändamålsenlig informationssäkerhet ska uppnås.

Gemensamt för de planerade åtgärderna är att de vid granskningstillfället inte är dokumenterade. Denna brist på definierade och avstämbara motiv, mål och metoder samt därtill hörande tidplaner gör det fortsatt osäkert om vilket ansvar IT-enheten har i förhållande till övrig verksamhet fram till att åtgärdsarbetena är färdigställda.

Med underlag av vår granskning vill vi särskilt uppmärksamma kommunstyrelsen på att så snart tillfälle ges:

- Redovisa hur de två övergripande åtgärdsarbetena ska utföras och ange när de kommer att vara färdigställda.
- Via sitt dataskyddsombud tydliggöra hur GDPR[1], dataskyddslagen och NIS-direktivet[2] ska efterlevas.

---

[1] *"Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)"* vanligtvis förkortat GDPR. Den 18 april 2018 fattade Riksdagen beslut om Dataskyddslagen som ett komplement till GDPR. I dataskyddslagen, förtydligas det bland annat under vilka förutsättningar vissa personuppgifter får behandlas. Dataskyddslagen tillåter att andra lagar som rör behandling av personuppgifter ändras och uppdateras i samband med införandet av GDPR. Lagändringarna gäller från den 25 maj 2018.

[2] *"Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen."* Från och med den 10 maj 2018 ställs nya krav inom EU på säkerhet i nätverk och informationssystem. De nya reglerna omfattar leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. De handlar bland annat om krav gällande säkerhetsåtgärder, incidentrapportering och tillsyn. Den 29 mars 2018 beslutade regeringen om propositionen Informationssäkerhet för samhällsviktiga och digitala tjänster (Prop. 2017/18:205). Den nya lagen föreslås träda i kraft den 1 augusti 2018.

2 Inledning/bakgrund

Vi har av Malung-Sälens kommuns revisorer haft i uppdrag att utföra en granskning av IT-enheten avseende organisation, uppdrag, resursförsörjning samt arbetsformer och rutiner. Uppdraget ingår i revisionsplanen för år 2018.

Informationsteknologi är ett vitt begrepp som omfattar större och större områden. Allt från det man i vanliga fall tänker på datorer, programvaror och skrivare. Men även delar som telefoner, passersystem, pedagogiska hjälpmedel och mycket annat. Informationsteknologi är därmed inte bara ett brett område utan också ett komplext område som får ett stort genomslag i form av 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.

Malung-Sälens kommuns revisorer utesluter inte att det finns risk för att den strategiska försörjningen och utvecklingen av verksamhetsstöd inte är ändamålsenlig.

2.1 Syfte, revisionsfråga och avgränsning

Syftet med granskningen är att bedöma om kommunen har säkerställt en sammanhållen, effektiv, ändamålsenlig och strategisk försörjning och utveckling gällande det verksamhetsstöd som en IT-enhet kan förväntas tillhandahålla.

Granskningen omfattar följande:

- Vilka styrande dokument i form av strategier, policys och därtill hörande tillämpningsföreskrifter finns för IT-enheten.
- IT-enhetens organisation, uppdrag och resursförsörjning.
- IT-enhetens arbetsformer och rutiner.
- Hur roller och ansvar fördelas inom enheten och med övrig verksamhet.
- Vem/vilka har rätt att teckna avtal.
- Hur IT-enheten finansieras.
- Hur uppfattar övriga verksamheter IT-enhetens stöd och support, samt inköp, installation och underhåll?

Granskningen avser kommunstyrelsen.

2.2 Revisionskriterier

Vi har bedömt om verksamheten:

- Efterlever kommunallagen 6 kap. 6 §
- Har och efterlever beslutade interna regelverk samt policys med därtill hörande tillämpningsföreskrifter

2.3 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer.

Rapporten är faktakontrollerad av IT-chefen.

3 Resultat av granskningen

Granskningen är utförd i flera steg. Inledningsvis översändes intervjufrågorna, även innefattande förfrågan om kopior på styrande dokument, redovisade i bilaga 1. Erhållna svar är kompletterade med intervju av IT-chef och kommunchef 2018-06-29.

3.1 Styrande dokument

3.1.1 Allmänt

Enligt uppgift så finns det inga dokumenterade IT-strategier för vare sig kommunen som helhet eller för IT-enheten. IT-enheten uppges arbeta efter "muntlig tradition" då det även saknas en dokumenterad uppdragsbeskrivning. Vad gäller systemförvaltning så hänvisas till, men redovisas inte, IT-enhetens dokumentation av det lokala nätverket.

De enda styrdokument vi erhållit avser informationssäkerhet och består av en tio år gammal oreviderad policy med vidhängande tillämpningsföreskrifter.

Vid intervjun framkommer att det efter höstens val ska utarbetas en styrmodell för kommunen. Den uppges ska innefatta styrande dokument inklusive strategier för IT-verksamheten. Vid intervjutillfället finns inga projektdokument eller motsvarande som beskriver mål, metoder, medarbetare och tidplan för arbetet. Med andra ord fanns vid intervjutillfället ännu inga uppgifter om inriktning för systemförvaltning och hur informationssäkerheten ska anpassas till senare tids hot, risker och externa regler.

Kommentar

Om verksamhetskrav styr IT-enheten så sker det idag inte på något enhetligt och väl känt sätt. Det finns med andra ord ingen adekvat styrning och därmed inget för verksamhetsansvariga att förhålla sig till för att säkerställa att datoriserade verksamhetsstöd införs och används på ett ändamålsenligt och säkert sätt.

Systemförvaltning innebär att skapa en modell för att säkerställa att IT-enheten stödjer, underhåller och över tid vidareutvecklar verksamhetens uttryckta behov av systemstöd och tjänster. För att IT-enheten ska kunna göra detta krävs en beskrivning om vad som ska förvaltas. Med andra ord; IT-enheten behöver styrning om vad som skall göras och hur ansvar och arbetsuppgifter ska fördelas mellan dem och kärnverksamheten. En inom kommunen nödvändig samsyn om sambanden mellan krav, förväntningar och kostnader ger den lika nödvändiga förståelse som ökar den faktiska kvaliteten på vad en IT-enhet levererar.

Vad gäller informationssäkerheten hämtar vi vår kommentar och rekommendationer från MSB[3]: s site. *"Kommunerna har ett av det svenska samhällets mest komplexa*

[3] Myndigheten för samhällsskydd och beredskap

uppdrag. Det omfattar allt från den dagliga omsorgen av äldre till att säkerställa att känslig infrastruktur fungerar. En stor del av den samhällsviktiga verksamheten räknas till kommunernas ansvar. I samtliga delar av uppdraget spelar säker informationshantering en central roll." I bilaga 2 redovisas MSB: s kortfattade rekommendationer i åtta punkter[4] om hur en kommun kan agera för att uppnå en ändamålsenlig informationssäkerhet.

Det är väsentligt att den styrmodell som aviseras ska införas hanterar detta.

3.1.2 GDPR och NIS-direktivet

"Uppdrag att inventera och upprätta ett register över it-enhetens system" är det svar vi erhållit på våra frågor om vad IT-enheten haft och framgent har avseende rubricerat.

Svaret kompletteras vid intervjun med att kommunens dataskyddsombud tillsammans med verksamhetsansvariga och extern konsult ska starta ett arbete med att klassificera den information kommunen hanterar. Det ska i sin tur leda till nya styrdokument avseende informationssäkerhet som i förlängningen ska leda till att GDPR och NIS-direktivet kan efterlevas. IT-enheten säger sig vara involverad och förvaltningarna uppges vara muntligen informerade om vad som ska ske innefattande deras medverkan. Vid intervjutillfället finns dock inga projektdokument eller motsvarande som beskriver mål, metoder, medarbetare och tidplan för arbetet.

Fram till att projektet påbörjas gör vi bedömningen att IT-enheten inte fått några dokumenterade instruktioner om vad verksamhetsansvariga förväntar sig att de ska ansvara för så att kommunen som helhet ska ha möjlighet att efterleva de nya externa regler som gäller med början från första halvåret 2018.

Kommentar

Innan åtgärdsarbetet slutförts utesluter vi inte att det föreligger signifikanta brister i kommunens förmåga att efterleva under 2018 nytillkomna förordningar, direktiv och lagar inom de områden där IT-enheten rimligtvis har en ansvarsroll att fylla.

Av protokollet daterat 2018-05-22 från sammanträdet i Kommunstyrelsens arbetsutskott framgår att kommunen utnämnt ett dataskyddsombud. Dataskyddsombudet har som framgår av protokollet *"en kontrollerande och rådgivande funktion"*.

Vi anser att ombudet, innan projektarbetet påbörjats, behöver överlämna de instruktioner som IT-enheten har att förhålla sig till för att säkerställa efterlevnaden av GDPR och dataskyddslagen inom sitt ansvarsområde. För att säkerställa efterlevnad av NIS-direktivet rekommenderas att verksamhetsansvariga tillsammans med IT-enheten inhämtar information från de tillsynsmyndigheter[5] som är aktuella för kommunen.

[4] Eftersom behovet av en ständigt uppdaterad informationssäkerhet innebär att rekommendationerna kan förändrats över tid så redovisas här länken till där de redovisas.
https://www.msb.se/Upload/Forebyggande/Informationssakerhet/MSBRekommendationer_kommuner_korthet_170113.pdf

[5] Som exempel: Datainspektionen, MSB, Inspektionen för vård och omsorg (IVO) och Livsmedelsverket

3.2 Organisation, uppdrag och resursförsörjning

IT-enheten bemannas av chef samt fem tekniker varav tre är, som det uttrycks, uthyrda som *"skol-tekniker"*. Övriga två utgår från IT-enheten och stödjer förutom kommunen tre kommunala bolag. Vi har inte erhållit några specifika befattningsbeskrivningar.

Arbetsuppgifterna består sammantaget av som det uttrycks: *"IT-drift av servermiljö, nätverket ,E-post, AD, Spamfilter, backup, safecom printlösning, support av verksamhetssystem och användarsupport"* Till det även *"Telefonin avseende hårdvara"*.

Chefen för IT-enheten rapporterar *"vid behov"* till kommunchefen. Kommunikationen har enligt uppgift inte resulterat i att rapporteringen dokumenterats. Vi uppfattar av svaren att personal från IT-enheten inte regelmässigt och regelbundet medverkar i arbets-, samordnings- eller samverkansgrupper där andra medarbetare i kommunen ingår.

På frågan *"Är det IT-enhetens uppfattning att bemanning och kunskap möter de behov och krav som framställs av överordnad funktion och verksamheten i övrigt?"* svaras: *"Kunskapsmässigt JA, personalmässigt NEJ"*.

Det har de senaste två åren inte förekommit att det utförts någon form av undersökning/enkät ställd till verksamheten i övrigt om vad den anser om och önskar/kräver av IT-enheten.

Det finns ingen dokumenterad och fastställd utbildningsplan för IT-enheten. Det finns heller ingen en behovsanalys som underbygger en sådan.

Kommentar

Det som framgår av avsnittet understryker behovet av de åtgärder som rekommenderats ovan. Vad gäller organisationen är det här särskilt viktigt att det tydligt framgår var IT-personalen i ändamålsenligt antal organisationsmässigt placeras.

3.3 Arbetsformer och rutiner

På frågan om det finns etablerade och dokumenterade rutiner för: Återkommande driftåtgärder, säkerställd kontinuitet för vad som bedömts som verksamhetskritiska system och incidenthantering internt inom kommunen[6] och externt till myndigheter är svaret *"inget dokumenterat"*. Manuella rutiner/kontinuitetsplaner/katastrofplaner uppges inte ha testats de senaste två åren. IT-enheten upprätthåller inte vad som vanligtvis avses med en helpdeskfunktion. Tar IT-enheten hjälp från externt håll vänder man sig vid behov till ATEA[7]. Det framgår inte av svaret vilka anledningar som förekommer som leder fram till ett behov av stöd. Det framgår inte om stödet erhålls med underlag av en avtalad överenskommelse.

Det finns inget ärendehanteringssystem i drift som möjliggör att vi kan erhålla ett utdrag av händelser och åtgärder som IT-enheten utfört under 2018.

---

[6] Överordnade i linjen, politisk ledning, berörd verksamhet, anställda och kommunmedborgare.
[7] Atea uppger på sin site ha en bred avtalstäckning inom offentlig sektor genom ramavtal upphandlade av Statens Inköpscentral vid Kammarkollegiet (SIC) och SKL Kommentus Inköpscentral (SKI). a den offentliga sektorn kan även kommuner och landsting ansluta sig till ramavtalen inom området it och telekommunikation.

Kommentar

Det som framgår av avsnittet understryker ytterligare behovet av de åtgärder som rekommenderats ovan. IT-enheten bedriver sin verksamhet renons på styrande dokumentation. Det i sin tur innebär att kommunens IT-verksamhet till väsentlig del inte är möjlig att känna till för andra än IT-enheten eller de som har regelbunden detaljerad muntlig kontakt med dess företrädare. När nödvändiga åtgärder planeras och genomförs är det väsentligt att det tydliggörs för hela organisationen vem som styr vem och vad samt hur och varför.

3.4 Hur fördelas roller och ansvar inom IT-enheten och med övrig verksamhet

Enligt uppgift från IT-enheten så består samarbetet av att de ger allmän support till användare och till systemansvariga/-förvaltare för verksamhetssystem i kommunen och de fyra bolagen. Det är IT-enhetens uppfattning att samarbetet *"funkat bra"*.

Kommentar

Av de svar vi får på våra frågor så tolkar vi det så att några avtal (SLA)[8] mellan IT-enheten och verksamhetsansvariga inte finns upprättade. Vi anser att upprättande av sådana blir en naturlig konsekvens av de åtgärder vi rekommenderar ovan. Av vad som framkommit i tidigare avsnitt så har kommunen inte använt någon särskild metod för att klassificera den information som de olika verksamhetssystemen hanterar. Om det kan förutsättas att inventerings- och åtgärdsarbetet inför införandet av GDPR är grundligt utfört så finns där rimligen redan delar av nödvändig kunskap om hur olika informationstillgångar har klassificerats. Sveriges Kommuner och Landsting (SKL) tillhandahåller gratisverktyget KLASSA[9] för detta viktiga och nödvändiga grundarbete för att nå en ändamålsenlig informationssäkerhet. Vid intervjutillfället uppgavs att KLASSA är den metod som ska användas i kommande åtgärdsarbete.

3.5 Vem/vilka som har rätt att teckna avtal

På frågan: Under vilka omständigheter och för vad har vem/vilka på IT-enheten rätt att (ska) teckna avtal med externa leverantörer av varor och/eller tjänster svaras: *"IT-chef till inköp för den 'dagliga' driften enligt budget"*. Enligt erhållen delegationsordning antagen av kommunstyrelsen och daterad 2014-03-11 är IT-chefen en så kallad stabschef med ansvar *"för den operativa driften"* för sin enhet. Det innebär att han kan *"beställa från gällande ramavtal (göra avrop)"* och *"genomföra direktupphandlingar (objektupphandlingar) upp till max 15 % av tröskelvärdet inklusive tilldelningsbeslut och kontraktstecknande"*. Femton procent av tröskelvärdet[10] innebär en beloppsgräns på

[8] Service Level Agreement eller på svenska Service Nivå Överenskommelse (SNÖ). Kan ses som en garanti i form av ett avtal där IT-enheten tillhandahåller en överenskommen kvalitet och innehåll på drifttjänsten till system-/objektsägaren. Ägaren utgår här från de behov som framkommer när informationen som systemet hanterar klassificeras.

[9] Informationsklassning är en metod som hjälper verksamheten att välja rätt åtgärder som skyddar informationen. För att förenkla kommuners, landstings och regioners genomförande av informationsklassningen har SKL tagit fram och underhåller verktyget KLASSA.

[10] Gränsen för direktupphandlingar höjdes 1 januari 2018 till 586 907 kr. De nya tröskelvärdena gäller för åren 2018 och 2019 och att de ska tillämpas på anbudsförfaranden som inleds efter 1 januari 2018.

88 000 kronor. Detta belopp per leverantör och år uppges inte överskridas för inköp *"för den 'dagliga' driften."*

Under 2018 uppges det planeras för inköp av datorer till skolan och för system för kommun- och/eller enhetsgemensamt administrativt system. Nytt IT-partneravtal ska avropas/upphandlas. Vid intervjun framkommer att det inte är IT-chefen som tecknar dessa avtal. Det gör inköps- och/eller kommunchef.

3.6 Enhetens finansiering

Erhållna budgetvärden framgår av bilaga 3. Budgeten uppges vara upprättad av IT-chef vilken vid intervjun också meddelar att han följer upp utfallet. Mottagare av fortlöpande avstämningarna uppges vara ekonomienheten.

Specificeringar i form av analyser och beräkningar uppfattar vi inte finnas dokumenterade. Förklaringarna till budgetposterna som lämnas är ofta uppskattningar med och utan koppling till utfallet 2017. Löner och sociala avgifter är uppräknade med tre procent från 2017 års nivå. Det finns även kostnader som uppges kända från ingångna avtal. Majoriteten av intäkterna *("Försäljning Verksamhet")* och köp av interna tjänster förklaras med "interna ersättningar". I erhållet underlag redogörs inte för hur dessa beräknas och vilka som debiteras vad och varför.

Vid intervjun framkommer detaljer om budgeten för 2018:

- Ramen på 1,3 MSEK är efter för kommunen allmänt sänkta budgetbelopp.
- Försäljning IT är debitering av inköp gjorda för de kommunala bolagen.
- Verksamhetsintäkter för tele är fördelning av fasta och rörliga abonnemangskostnader. Här ingår inte de ca 200 mobiltelefoner som inte är knutna till kommunens växel. Kostnaden för dessa tas av respektive förvaltning.
- I verksamhetsintäkterna IT ingår en interndebitering på 4 500 kronor per år och dator för kommunens 385 datorer.

Kommentar

Intäkter och kostnader med signifikant påverkan på budgeten ska rimligtvis över tid kunna kontrolleras vara korrekt beräknade. Förändringar av förutsättningarna för hur priserna kalkyleras och debiteras behöver kunna härledas inte minst för de som betalar och säkerställer att leveranserna överensstämmer med vad som avtalats. Vi rekommenderar att även detta blir tydligt i den kommande styrmodellen.

2018-10-03

KPMG AB

Lars Anteskog
Projektansvarig

Marita Castenhag
Kundansvarig

Malung-Sälens kommun
Granskning av IT-enheten
Bilaga 1 Intervjufrågor
2018-10-03

Allmänt

Finns dokumenten som efterfrågas nedan behöver vi få ta del av dem innan intervjutillfället. Om dokumenten är under framtagande så uppskattar vi att få ta del av senaste utkastet/arbetsexemplaret. Om det är så att dokument saknas men det finns planer på hur och när de ska upprättas behöver vi ta del av de planeringsdokument som beskriver detta. Om dokument saknas och någon planering ännu inte är genomförd önskar vi få uppgift om detta innan intervju.

Det går bra att skriftligen helt eller delvis svara på frågorna innan intervju. Använd när så önskas vår numrering.

Vilka styrande dokument i form av policys och riktlinjer finns för IT-enheten?

1. Finns det en IT-strategi (innefattande strategier för e-tjänster) för kommunen?
2. Finns det en strategi för IT-enheten?
3. Finns det en uppdragsbeskrivning för IT-enheten?
4. I eventuell avsaknad/inte ännu fastställda/planering av strategier och uppdragsbeskrivning vilka styrdokument anser IT-enheten att man verkar utifrån?
5. Finns det systemförvaltningsplaner (baserad på pm3, ITIL eller egenutvecklad organisation) för de datoriserade verksamhetsstöd kommunen använder?
6. Oavsett om det finns systemförvaltningsplaner eller inte finns det en systemförteckning som redovisar driftsatta system där det framgår vem som innehar de ansvar som identifierats?
7. Finns det en modern (med ett beslutsdatum inte äldre än fem år) informationssäkerhetspolicy för kommunen med tillhörande tillämpningsföreskrifter?
8. Finns det ett ledningssystem för informationssäkerhet (LIS) infört eller planerat?
9. Är LIS certifierat eller finns det planer på att certifiera sig efter ISO 27000-serien?
10. Oavsett styrande dokument eller inte finns det i någon omfattning en informationsklassning utförd och på vilket sätt har den påverkat de IT-säkerhetsåtgärder som IT-enheten infört?
11. Finns det servicenivåöverenskommelser (SLA) mellan IT-enheten och verksamhetsansvariga? På vems/vilkas initiativ är de framtagna. Vi önskar får ett exempel på ett SLA.
12. Oavsett om det finns en modern informationssäkerhetspolicy eller inte, vilket ansvar anser/upplever IT-enheten sig ha för informationssäkerheten (kommunen i allmänhet och IT-enheten i synnerhet) och IT-säkerheten? Finns detta ställningstagande motiverat, dokumenterat och kommunicerat? Vem/Vilka har mottagit ställningstagandet och vilken respons/reaktion har erhållits?

13. Både NIS-direktivet och GDPR gäller från och med första halvåret 2018. Vilka instruktioner/uppdrag/ansvar har IT-enheten erhållit för att anpassa sin verksamhet för att säkerställa efterlevnad för kommunen i allmänhet och IT-enheten i synnerhet?
14. I eventuell avsaknad av instruktioner/uppdrag/utpekat ansvar vilka åtgärder har IT-enheten utfört för att efterleva NIS-direktivet och GDPR? Finns det dokumenterade bedömningar om eventuella brister som kan innebära skada (verksamhet och/eller ekonomisk) för kommunen? Finns det en brist- och/eller prioriteringslista där det framgår vad som eventuellt ännu inte åtgärdats, vilka konsekvenser det kan få och när samt när de planeras vara åtgärdade?
15. Har IT-enheten tagit stöd/involverats av kommunens dataskyddsombud (ett eller flera) under anpassningen till GDPR?

IT-enhetens organisation, uppdrag och resursförsörjning.

16. Hur är IT-enheten organiserad? Antalet medarbetare och deras arbetsuppgifter/ansvar. Finns det befattningsbeskrivningar eller motsvarande att ta del av?
17. Bortsett vad som omfrågats i avsnittet om styrande dokument ovan finns det något ytterligare att tillägga om IT-enhetens uppdrag.
18. Vem/Vilka rapporterar IT-enheten till? Med vilken periodicitet? Finns rapporteringen dokumenterad vill vi erhålla ett exempel. I vilka grupperingar (arbetssamordning-, samverkans- etc.) medverkar personer från IT-enheten?
19. Är det IT-enhetens uppfattning att bemanning och kunskap möter de behov och krav som framställs av överordnad funktion och verksamheten i övrigt?
20. Har det utförts någon form av undersökning/enkät ställd till verksamheten i övrigt om vad den anser om och önskar/kräver av IT-enheten? Om en undersökning gjorts de senaste två åren behöver vi frågorna, uppgift om svarsfrekvensen och de slutsatser IT-enheten drar av svaren. Vilka åtgärder har eventuellt utförts/startats eller planeras att starta med anledning av undersökningsresultat?
21. Finns det en dokumenterad och fastställd utbildningsplan för IT-enheten och är den fullföljd? Finns det en behovsanalys som underbygger utbildningsplanen och är andra än IT-enhetens personal involverade i analys, prioriteringar och beslut?

IT-enhetens arbetsformer och rutiner.

22. Finns det etablerade och dokumenterade rutiner för:
    a. Återkommande driftåtgärder?
    b. Säkerställd kontinuitet för vad som bedömts som verksamhetskritiska system?
    c. Incidenthantering som innefattar rapportering till överordnade, politiken, berörd verksamhet, anställda och kommunmedborgare?

d. Incidenthantering som innefattar rapportering till berörda myndigheter så som Datainspektionen (Integritetsskyddsmyndigheten), Myndigheten för samhällsskydd och beredskap (MSB).

23. Upprätthåller IT-enheten en helpdeskfunktion?
24. Vilka helpdesktjänster erbjuds?
25. Vilka "andra" och "tredje" linjens stöd kan/får/har man avtal att hänvisa till?
26. Finns det ett ärendehanteringssystem i drift som även möjliggör att vi kan erhålla ett utdrag av händelser och åtgärder under 2018?
27. Har manuella rutiner/kontinuitetsplaner/katastrofplaner testats de senaste två åren?

Hur roller och ansvar fördelas inom enheten och med övrig verksamhet.

28. Med vilka, om vad och hur är samarbete med övrig verksamhet organiserat 2018?
29. Hur upplever IT-enheten vad verksamheten anser om de samarbetsformer som används/använts?

Vem/vilka som har rätt att teckna avtal.

30. Under vilka omständigheter och för vad har vem/vilka på IT-enheten rätt att (ska) teckna avtal med externa leverantörer av varor och/eller tjänster?
31. Anser IT-enheten att interna och externa regler (lagen om offentlig upphandling) efterlevs när inköp görs?
32. Har det startas någon upphandling under 2018? Planeras eller pågår någon?
33. Vi behöver en kopia av delegations-/attestordning.

Hur finansieras IT-enheten?

Uppställningen till höger är ett enklare allmänt exempel på hur en budget för en IT-enhet kan redovisas. Utifrån den:

34. Finns det en budget för 2018 som är uppställd på detta eller på något annat sätt?
35. Vilka specificeringar i form av analyser och beräkningar har dokumenterats och kan redovisas för de budgetposter som redovisas i budgeten?
36. Vem/vilka har medverkat i upprättandet?
37. Dokumenterar IT-enheten uppföljningar och gör prognoser?

IT-enheten totala budget 20XX

	Budget 20XX
Försäljning (tjänster)	
Summa Intäkter	**- kr**
Personalkostnader inkl PO	*- kr*
Övriga perosnalkostnader	*- kr*
Köp av verksamhet	
Övriga verksamhetskostnader	
Kapitalkostnader	
Summa Kostnader	**- kr**
Totalsumma	**- kr**

	Investeringar 20XX
Projekt 1	
Projekt 2	
Projekt 3	
Totalsumma	**- kr**
Total budget 20XX	**- kr**

38. Vem/vilka rapporterar med vilken periodicitet uppföljningen av budgeten till vem/vilka?	

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

39. Täcks av fråga 20 ovan.

Malung-Sälens kommun
Granskning av IT-enheten
Bilaga 2 MSB: s rekommendationer avseende informationssäkerhet
2018-10-03

Utse en funktion för informationssäkerhet. Funktionens placering bör vara direkt underställd den högsta ledningen (kommunledningskontoret). Alternativt undersök möjligheten att samarbeta med närliggande kommuner och utse en gemensam funktion för informationssäkerhet. För att på bästa sätt kunna arbeta med frågorna visar erfarenhet att funktionen behöver använda en majoritet av sin tid till informationssäkerhetsuppdraget. Funktionen behöver kontinuerligt kompetensutvecklas och det är även betydelsefullt att samverkan sker med andra aktörer inom informationssäkerhetsområdet för att hålla sig uppdaterad samt utbyta erfarenheter.

Det första funktionen bör göra är att **ta fram en analys av nuläget i kommunen**. Gör en övergripande verksamhetsanalys för att få kunskap om organisationens processer, vilken information som hanteras, samt vilket behov av skydd och vilka krav som finns. Gör därefter en övergripande analys för att få en bild av riskerna kopplade till den information som hanteras. Gör också en gap-analys genom en inventering av existerande säkerhetsåtgärder jämförda med skyddsbehovet som framkommit genom verksamhets och riskanalysen. Här handlar det om att skapa en samlad bild av informationssäkerhetsnivån i kommunen. Detta blir ett viktigt underlag för ledningsbeslut.

Informera ledningen hur nuläget ser ut. Visa exempel på reella hot och inträffade incidenter. Beskriv några centrala lagkrav, t.ex. dataskyddsförordningen, som får stor påverkan på hur kommunen hanterar personuppgifter. Visa på förutsättningarna för säker digitalisering etc. Informationssäkerhetsområdet är ett komplext område och flera kompetenser behövs i arbetet.

Skapa en handlingsplan utifrån nuläget. Handlingsplanen bör beslutas av ledningen. Ta fram styrdokument, policy och riktlinjer samt åtgärda de viktigaste bristerna och sårbarheterna, t.ex. beredskap mot skadlig kod, backuprutiner etc. MSB rekommenderar kommunerna att ta fram en gemensam struktur på styrdokument för informationssäkerhetsområdet.

Identifiera vilken information som hanteras i verksamheten. **Klassa sedan informationen** efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet. Fokusera på den mest kritiska informationen/känsliga informationen som är i behov av höga skyddskrav. Ta gärna hjälp av *Metodstöd för LIS* på Informationssakerhet.se samt SKL:s verktyg *KLASSA*.

Ta fram styrdokument. **Se till att höja säkerhetsmedvetandet inom kommunen** och ge stöd till organisationens förmåga att efterleva kraven i framtagna riktlinjer. Detta kan ske t.ex. genom utbildning, att ta fram vägledningar och annan information.

Ta fram informationssäkerhetsrelaterade krav som sedan används vid upphandlingar. Se till att identifiera informationssäkerhetskraven samt etablera en process för att få med kraven i upphandlingar.

Gör uppföljningar. Se över om kommunen efterlever det som står i de framtagna riktlinjerna. Planera in återkommande uppföljning/revison av verksamheten. Resultaten av uppföljning ska ingå som en del av den återkommande rapporteringen till ledningen.

Malung-Sälens kommun
Granskning av IT-enheten
Bilaga 3 Budget för 2018
2018-10-03

	Budget IT-enheten	IT	Tele	Ansvar 15	Specificering
	Ram			1 300	
30	Försäljning	550	0	550	Uppskattning
36	Försäljning Verksamhet	7 640	1 075	8 715	Interna ersättningar
	Summa intäkter IT	**8 190**	**1 075**	**10 565**	
48	Köp av entreprenad	250			Interna ersättn enl uppgift från ekonomienheten
50	Lön arb. Tid	2 016			Upp 3 % från fg år
51	Lön ej arb. Tid	275			Upp 3 % från fg år
55	Kostnadsersättning	125			Utfall 2017
56	Sociala avg.	910			Upp 3 % från fg år
60	Hyror och fastighet	190			Samma som för 2017
61	Fast. Entreprenad	60			Uppskattning/2017
63	Leasing	152			Enl avtal
64	Förbruknings mtrl.	500	10	510	Uppskattning/2017
65	Kontors material	185			Uppskattning/2017
68	Tele och Datakom	1 100	854	1 954	Uppskattning/2017/Aktuella kostn Tele
69	Kostnad för transport	10			Uppskattning/2017
70	Transport och resor	35			Uppskattning/2017
71	Personal-representation	10			Uppskattning/2017
72	Annonser	5			Uppskattning/2017
74	Div främmande tjänster	2 946	477	3 423	Enl avtal/Uppskattning av konsulttj./Plan för fiber
76	Div kostnad	135	20	155	Uppskattning/2017
79	Avskrivning	300			Enl plan
	Summa Utgifter IT	**9 204**	**1 361**	**10 565**	